HP OpenView

Storage Mirroring user’s guide

Storage Mirroring Application Manager

Part number: T2558-96005
Fourth edition: September 2006

Legal and notice information

The information contained herein is subject to change without notice. The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

Printed in the US

Table of Contents

About this guide

This document describes how to use the Storage Mirroring® Application Manager interface to create and validate your application configuration.

Related documentation

Before you begin to configure your solution, make sure that you have complete documentation for your operating system, application, and Storage Mirroring.

User's guide

The following document(s) contain additional information that you may need while setting up this solution:

- Storage Mirroring *User's Guide* or online documentation

Application notes

While the Storage Mirroring Application Manager greatly simplifies the process of configuring your application for use with Storage Mirroring, Hewlett-Packard recognizes that in some environments a manual process for application configuration is more desirable. However, the manual process is much more time consuming and labor intensive. Hewlett-Packard has application notes which provide guidelines on using manual processes to configure your application with Storage Mirroring.

To obtain application notes for the manual process for Exchange configurations, you must contact Hewlett-Packard technical support. Current contact information for technical support is available at `http://www.hp.com/support/`.

Application notes for using SQL are available for download from the Application Notes page of the Hewlett-Packard support web site (`http:/www.hp.com/support/manuals.`).

Readme files

The following readme files contain additional reference information related to the Storage Mirroring Application Manager:

- `Readme_Application_Manager.htm`—The readme file contains information about known issues and workarounds in the current release of the Application Manager.
- `Readme_DFO.htm`—The DNS failover utility (`DFO.exe`), which is called in the failover scripts, automatically updates DNS resource records in order to seamlessly redirect network clients. The DFO readme file documents DFO syntax, known issues, and workarounds.

The readme files can be found in the folder where the Storage Mirroring Application Manager is installed (the default installation location is either `\Program Files\Storage Mirroring\` or `\Program files\Application Manager`.)

HP technical support

For worldwide technical support information, see the HP support website:

`http://www.hp.com/support`

Before contacting HP, collect the following information:

- Product model names and numbers
- Technical support registration number (if applicable)
- Product serial numbers
- Error messages
- Operating system type and revision level
- Detailed questions

Customer self repair

HP customer self repair (CSR) programs allow you to repair your StorageWorks product. If a CSR part needs replacing, HP ships the part directly to you so that you can install it at your convenience. Some parts do not qualify for CSR. Your HP-authorized service provider will determine whether a repair can be accomplished by CSR.

For more information about CSR, contact your local service provider. For North America, see the CSR website:

`http://www.hp.com/go/selfrepair`

Product warranties

For information about HP StorageWorks product warranties, see the warranty information website:

`http://www.hp.com/go/storagewarranty`

Subscription service

HP recommends that you register your product at the Subscriber's Choice for Business website:

`http://www.hp.com/go/e-updates`

After registering, you will receive e-mail notification of product enhancements, new driver versions, firmware updates, and other product resources.

HP websites

For additional information, see the following HP websites:

- `http://www.hp.com`
- `http://www.hp.com/go/storage`
- `http://www.hp.com/service_locator`
- `http://www.hp.com/support/manuals`
- `http://www.hp.com/support/downloads`

Documentation feedback

HP welcomes your feedback.

To make comments and suggestions about product documentation, please send a message to `storagedocs.feedback@hp.com`. All submissions become the property of HP.

Introduction

This document describes how to use the Storage Mirroring Application Manager interface to create and validate your application configuration. The Application Manager lets you quickly configure protection for an application without requiring you to have advanced knowledge of either Storage Mirroring or your application. The Application Manager works by gathering information about your source and target environments, then configuring Storage Mirroring to protect the source.

About the Storage Mirroring® Application Manager

The Storage Mirroring Application Manager is used to simplify the setup of standard Storage Mirroring connections. The Application Manager discovers all servers running a designated application in your environment so that you can determine which servers are not protected. It gathers information about the environment from various sources (including Storage Mirroring, Active Directory®, and DNS) and automatically configures Storage Mirroring to protect that environment. It also performs a “health check” to make sure that your configuration is correct. This check not only helps to reduce configuration errors, but it also simplifies the setup process.

Using the Storage Mirroring Application Manager with Exchange in clustered environments

The Storage Mirroring Application Manager can be used in the following cluster configurations with Exchange:

- Multi-node cluster to another multi-node cluster

NOTE: Both the source and target servers **MUST** to be clustered in order to use the Storage Mirroring Application Manager to configure and manage clustered Exchange servers.

Using the Storage Mirroring Application Manager with SQL in clustered environments

The Storage Mirroring Application Manager is intended to be used for one-to-one configurations in non-clustered SQL environments.

If you want to use SQL in a clustered environment, refer to one of the following application notes, available from `http:/www.hp.com/support/manuals.`:

- *Guidelines for using Microsoft SQL Server 7.0 with Storage Mirroring*
- *Guidelines for using Microsoft SQL Server 2000 with Storage Mirroring*
- *Guidelines for using Microsoft SQL Server 2005 with Storage Mirroring*

Requirements

The Storage Mirroring Application Manager will run from any client (or server) on any Microsoft® Windows® operating system that has access to the domain in which the servers are located.

The Storage Mirroring Application Manager requires the following minimum system configuration:

- Two servers that meet one of the following operating system requirements:
  - Microsoft Windows 2000 Service Pack 4 or later
  - Microsoft Windows 2003

  NOTE: In order to use the Target Data Verification feature (available only for Exchange), the target must be running Windows 2003 server, Service Pack 1.

- Two licensed copies of Storage Mirroring version 4.4.2 or later
- A copy of the most recent version of the Storage Mirroring Application Manager

  NOTE:
  - To avoid having to install unnecessary software on your production source or target servers, you should install and run the Storage Mirroring Application Manager on a Windows XP client within the domain.
  - See the Hewlett-Packard support website to obtain the most recent version of the Storage Mirroring Application Manager.

- .NET Framework version 2.0 or later. If you do not have .NET Framework version 2.0 installed, Application Manager will prompt you to install it
- Microsoft Installer version 3.0 or later (as required by the .NET Framework version 2.0)
- An active internet connection (required during the Storage Mirroring Application Manager installation in order to download the Microsoft Admin Pack and/or SQL Server 2005 Backward Compatibility components containing the SQLDMO libraries)
- If the DNS server is running Windows Server™ 2000, you must have the DNS Windows Management Instrumentation (WMI) Provider installed on the source's primary DNS server to allow the DFO to modify DNS resource records during failover. To download the DNS WMI Provider, use the following link:

  `ftp.microsoft.com/reskit/win2000/dnsprov.zip`

In addition, your environment must adhere to requirements specific to the application you are protecting. For additional requirements, see Exchange Manager requirements, page 8 or SQL Manager requirements, page 8.

Exchange Manager requirements

If you are using the Storage Mirroring Application Manager for Exchange, your system must meet the following requirements:

- Two licensed copies of Microsoft Exchange Server that meet one of the following requirements:
  - Exchange Server 2000 with Service Pack 3 or later
  - Exchange Server 2003

NOTE:
- Hewlett-Packard recommends that the Exchange version be the same as the operating system version (for example, Windows Server 2000 running Exchange Server 2000, or Windows Server 2003 running Exchange 2003).
- The source and target servers must both be running a Microsoft-supported operating system/Exchange combination.
- Both source and target Exchange versions must be identical.

- To use the Storage Mirroring Application Manager for Exchange, Storage Mirroring must be running under the `localsystem` account.
- The client or server that is running the Application Manager must have access to the domain in which the Exchange servers are located.
- The source and target servers must be part of the same Exchange Administrative Group.
- The Exchange servers must have the same root domain.
- While installing Exchange Server 2003 on a domain controller is a supported operation, it is not generally recommended. Hewlett-Packard also does not recommend this configuration. If you must use Exchange Server 2003 on a domain controller, review the following Microsoft Knowledge Base articles:

  ```
  http://support.microsoft.com/kb/822179
  http://support.microsoft.com/kb/822575
  http://support.microsoft.com/kb/332097
  http://support.microsoft.com/kb/305065
  http://support.microsoft.com/kb/304403
  http://support.microsoft.com/kb/875427
  ```

SQL Manager requirements

If you are using the Storage Mirroring Application Manager for SQL, your system must meet the following requirements:

- Two licensed copies of Microsoft SQL Server that meet one of the following requirements:
  - SQL Server 2000 with Service Pack 3 or later
  - SQL Server 2005

NOTE: If you are using SQL Server, you will be prompted to download and install the Microsoft SQL Server 2005 backward compatibility components. This package includes the SQLDMO library, which is required to run the Application Manager.

- To use the Storage Mirroring Application Manager for SQL, the user logged on to Windows **must** be a member of the SQL Server `sysadmin` role on the source and target servers.
- The source and target SQL servers **must** be in the same domain; otherwise, the SQL Server service on both the source and target servers must be configured to start with the same domain user account.

What’s new in version 4.1

The Storage Mirroring Application Manager version 4.1 includes new features, most notably the addition of support for protecting SQL servers and for protecting clustered Exchange servers.

Refer to the readme file (`Readme_Application_Manager.htm`) for information about known issues and workarounds in the current release.

You can now use the Application Manager to:

- Configure support for Exchange clusters
- Select Exchange Storage Groups to protect
- Perform disaster recovery testing for Exchange
- Protect SQL servers
    - Discover, set up, and perform integrated failback and restoration
    - Select to protect a default SQL instance or a database
- Configure compression settings to be used during restoration
- Select or specify the DNS server to update
- Manage and monitor protected servers from within the Storage Mirroring Application Manager

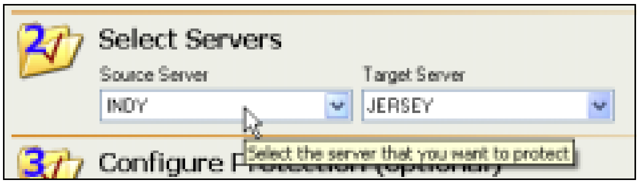
Navigating the user interface

The Application Manager interface is designed to guide you through the process of configuring protection for your servers. The default configuration parameters have been selected to be appropriate for most configurations; however, they may need to be modified for your specific environment. Any changes you make to non-machine specific configuration settings (such as Missed Packets) will become the default the next time you run the Application Manager.

When you launch the Application Manager, you will see the main Application Manager window. The Setup tab of the Application Manager window leads you through the steps to configure protection for a server using standard Windows-style controls. Enter information in fields, select options from drop-down menus, click buttons, and use menu options to configure protection.

After protection has been set up, use the Monitor tab to view information about the current source/target pair. Based on the current protection status and/or failover state, the Failover, Monitoring, and Protection button text on the Monitor tab will be updated to display the available command. If the Application Manager is not in a state that will allow any of these options to be executed, the corresponding button(s) will be grayed out (disabled).

The interface provides tooltip-style online help. When you place the pointer over a field in the Application Manager, a tooltip will appear to provide additional information about the field.



2 Select Servers

Source Server: INDY

Target Server: JERSEY

Select the server that you want to protect

3 Configure P

Install the Storage Mirroring Application Manager

If you have not done so already, install the Storage Mirroring Application Manager by running the Application Manager installation file downloaded from the Hewlett-Packard support website or from your installation media. If you install .NET during the Application Manager installation, you may be required to reboot your system prior to the installation of Application Manager. After the reboot, the installation should continue.

For the initial setup, the Storage Mirroring Application Manager only needs to be installed on one system. For managing failover and failback, the Application Manager should be run from either the target server or an administrative workstation.

NOTE: To avoid having to install unnecessary software on your production source or target servers, you should install and run the Storage Mirroring Application Manager on an administrative workstation within the domain.

The Storage Mirroring Application Manager installation requires an active internet connection. This is necessary in order to download the Microsoft Admin Pack and SQL server backward compatibility (SQLDMO) files. In addition, if you do not have .NET Framework version 2.0 installed, you will be prompted to install it. Microsoft Installer version 3.0 or later is required to install the .NET Framework.

Start the Storage Mirroring Application Manager

Launch the Application Manager by selecting **Start, Programs, Storage Mirroring, Application Manager**. Select **Exchange Manager** or **SQL Manager**, depending on the application you want to protect. The Storage Mirroring Application Manager will open. If you have not yet set up protection, the window will show the Setup tab for the application you selected. If you have previously configured protection for a source/target pair, the Application Manager will show the Monitor tab with information about the last protected pair.

You can protect servers for a different application by selecting one of the following options in the Tasks area on the left pane:

- **Protect Exchange Server**—To protect an Exchange server, click this option. The right pane will display the Manage Exchange page, which will lead you through the steps to protect an Exchange server. Continue with Protecting an Exchange Server, page 13.

- **Protect SQL Server**—To protect a SQL server, click this option. The right pane will display the Manage SQL page, which will lead you through the steps to protect a SQL server. Continue with Protecting a SQL Server, page 25.

Menu options

Based on the current protection status and/or failover state, the Protection, Monitoring, and Failover/Failback menu options will be updated to display the available command. If the Application Manager is not in a state that will allow any of these options to be executed, the corresponding menu option(s) will be grayed out (disabled).

The following menu options are available on the main Application Manager window:

File menu

- **New**—Select to protect an Exchange or SQL server
- **Exit**—Exit the Storage Mirroring Application Manager

Tools menu

- **Options**—Modify Storage Mirroring Application Manager display preferences

Actions menu

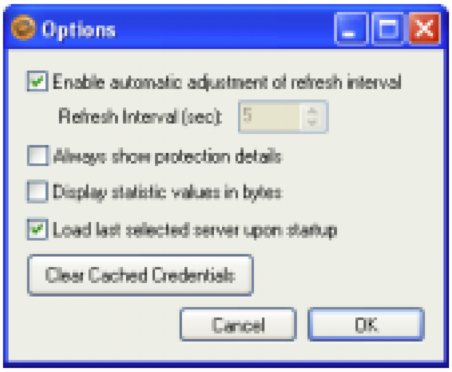
- **Configure Protection**—Launch the Configure Protection screen
- **Validate**—Validate the source/target configuration
- **Enable/Disable Protection**—Enable or disable protection for the source server
- **Enable/Disable Monitoring**—Enable or disable failover monitoring for the source server
- **Failover/Failback**—Initiate manual failover or failback
- **Manage SQL Servers** (SQL only)—Extended options for selecting SQL servers and testing SQL services on those servers This is the same window that is displayed when you click the **Advanced Find** button on the SQL Manager main page.
- **Verify Target Data** (Exchange only)—Verify that the target stores will mount with the replicated data without forcing a re-mirror

Help menu

- **View Online Help**—Launch the Storage Mirroring Application Manager online help
- **View User's Guide**—Launch the Storage Mirroring Application Manager *User's Guide* PDF
- **About**—View the Application Manager revision number and copyright information

Changing Storage Mirroring Application Manager preferences

To change display preferences for the Storage Mirroring Application Manager, select **Tools, Options**. The Options dialog box will appear.



☑ Enable automatic adjustment of refresh interval

Refresh Interval (sec): 5

□ Always show protection details

□ Display statistic values in bytes

☑ Load last selected server upon startup

To specify the rate at which the Application Manager updates the protection status, clear the **Enable automatic adjustment of refresh interval** checkbox, then enter the desired Refresh Interval. You can enter a value between 1 and 30,000 seconds.

If you want the refresh interval to be updated automatically, select the **Enable automatic adjustment of refresh interval** checkbox.

NOTE: If the Application Manager appears to be running slowly, it may be because the refresh interval is set to a long interval. Set a shorter refresh interval, and make sure that the automatic adjustment option is **not** selected.

To have the Protection Details section on the Monitor tab expanded by default, select the **Always show protection details** checkbox.

Select the **Display statistics values in bytes** checkbox if you always want to show these values in bytes, rather than in MB, GB, or TB.

If you want Storage Mirroring Application Manager to automatically reconnect to the last protected source/target pair when it is re-started, select the **Load last selected server upon startup** checkbox.

To clear the cached user name and password, click the **Clear Cached Credentials** button.

Click **OK** to save your changes, or **Cancel** to discard your changes and exit the **Options** dialog box.

Using the online help

To view additional information about a task in the Storage Mirroring Application Manager interface, from the **Help** menu, click **View Online Help**. This will launch the online help file in your internet browser.

To search for information about a topic, use tabs on the left pane:

- The **Contents** tab provides a table of contents for the help file. Click a topic to view the topic in the right pane.
- The **Index** tab provides a list of terms. Click on a term to view the help topic(s) that include that term.
- The **Search** tab allows you to enter a word or words. When you click the **Search** button, a list of all topics that include that term appears. Click on the topic title to view the topic.

NOTE: While viewing the online help and readme (.htm) files in Internet Explorer, a message may appear stating that Internet Explorer has restricted the file from showing active content. You can disable this setting by modifying your Internet Explorer security settings. In Internet Explorer, select **Tools, Internet Options**. On the **Advanced** tab, scroll down to the **Security** section, then enable **Allow active content to run in files on My Computer**.

Protecting an Exchange Server

Exchange configuration workflow

To configure protection for your Exchange servers using Application Manager, you will complete the following steps:

1. Install Storage Mirroring on the source and target Exchange servers. See the Storage Mirroring *Getting Started* guide for more information.
2. Install the Storage Mirroring Application Manager, page 10
3. Select a task, page 13
4. Select a domain, page 14
5. Select source and target servers, page 15
6. (Optional) Configure protection settings, page 16
7. Validate the Configuration, page 38

To protect your Exchange server, you will complete the following steps:

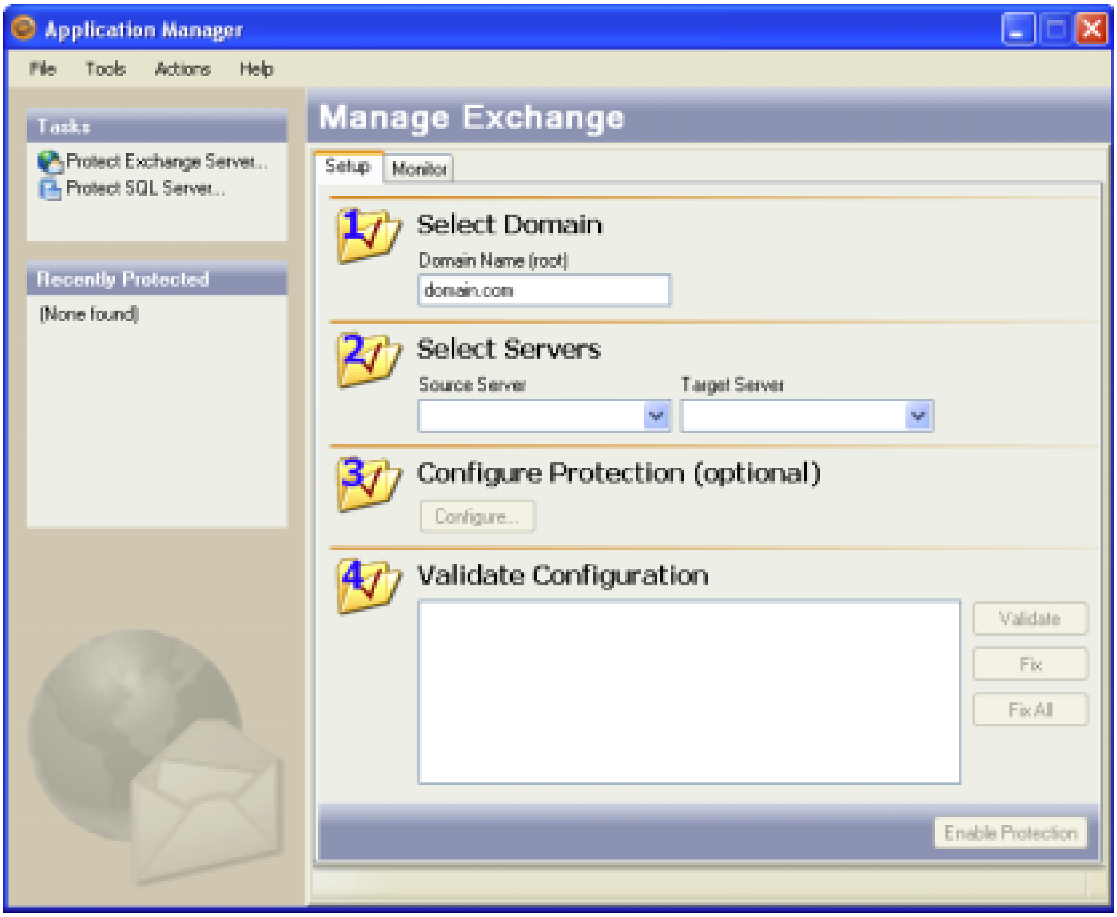
1. Enable protection, page 39
2. Monitor protection status, page 40

In the event of a failure, you will need to perform some additional tasks. These tasks are described in Failover, Failback, and Restoration, page 43.

Select a task

To protect an Exchange server, either open the Application Manager for Exchange (**Start, Programs, Storage Mirroring, Application Manager, Exchange Manager**), or from the Tasks area on the left pane, select **Protect Exchange Server**. The Manage Exchange page will appear in the right pane. Make sure that the Setup tab is in view.

If you have previously configured protection for a source/target pair, the Manage Exchange page will be populated with information about the protected pair.



Manage Exchange

1 Select Domain

Domain Name (root): domain.com

2 Select Servers

Source Server

Target Server

3 Configure Protection (optional)

4 Validate Configuration

(None found)

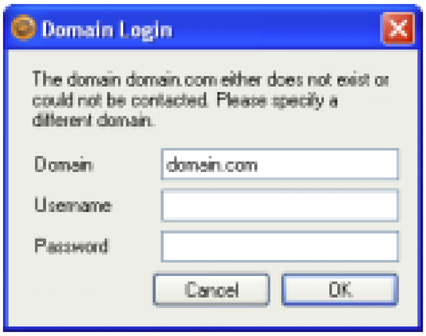
Select a domain

The **Domain Name** on the main window will be populated automatically with the root domain where the Application Manager client resides.

If you want to change the domain, type in a domain name for a trusted root domain that the Application Manager client can connect to, then press Tab or click on another field. If the domain you entered doesn’t exist or you do not have the credentials to modify Active Directory for the new domain, the Domain Login window will appear. You will be prompted to enter the domain name, user name, and password to use for logging in to the domain.

The user account should have **administrator** permissions. For more information about permissions, see Appendix A: Recommended Credentials, page 48.

You may enter a username for a different domain by entering a fully-qualified user name. The fully-qualified user name must be in the format **domain\username** or **username@domain**. If you enter a non-qualified name, the default domain will be used.



The domain domain.com either does not exist or could not be contacted. Please specify a different domain.

Domain: domain.com

Username:

Password:

NOTE: When the Storage Mirroring Application Manager launches, it selects the forest root automatically. The domain that is entered **MUST** be the root of the forest domain, since this is where all Exchange server objects reside (even if the Exchange server is a member of a child domain).

Select source and target servers

The Application Manager will automatically attempt to populate the **Source Server** and **Target Server** lists with any servers in the specified domain that are running Exchange.

If you select a source/target pair for which you have previously enabled and disabled protection, you may use the existing configuration settings (provided that the source/target connection is not currently active, in which case the existing settings will always be used). When you select **Configure** or **Validate**, a prompt will appear, asking if you want to re-use the previous configuration information. Click **Yes** to re-use the previous information, or click **No** to revert to the Application Manager default settings.

NOTE: If the IP address(es) for the source or target server have changed since you originally configured protection (for example, if you configure the source or target in a staging area and then send it to a production location), you must re-configure the protection settings. When you are prompted to re-use the previous protection configuration, click **No**, then click the **Configure Protection** button.

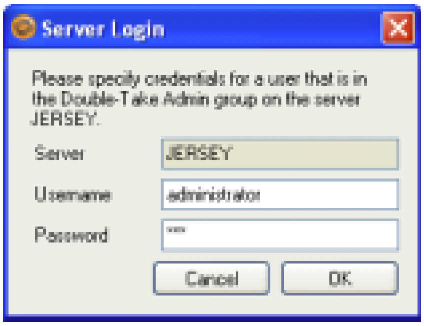
1. In the **Source Server** field, select the Exchange server that you want to protect. If this is your first time to log in to the selected server, you will be prompted to enter server login information. See Enter server login information, page 15 for more information about logging in to servers.
2. In the **Target Server** field, select the backup Exchange server that will protect the source server in the event of a failure. The target must be in the same Exchange admin group as the source.

Notice that after you select a server to protect, the Protection Status changes to “Unprotected”.

NOTE: If you select a target that is monitoring a connection that has met a failover condition and requires manual intervention, a prompt will appear, asking if you want to initiate failover.

Enter server login information

After you select a server for the first time, you will be prompted to enter a user name and password to use for logging in to the selected server. The login account **MUST** be a member of the Storage Mirroring Admin local security group for the selected server. For more information about permissions, see Appendix A: Recommended Credentials, page 48.



Please specify credentials for a user that is in the Double-Take Admin group on the server JERSEY.

Server: JERSEY

Username: administrator

Password: ***

You may enter a username for a different domain by entering a fully-qualified user name. The fully-qualified user name must be in the format **domain\username** or **username@domain**. If you enter a non-qualified name, the DNS domain will be used.

The Application Manager will attempt to use the same user name and password the next time you select a server.

Using clustered Exchange servers

Exchange virtual servers are selectable in the same way as physical servers. The physical servers belonging to a cluster are not shown in the server drop-down lists.

Configure protection settings

If you do not need to change the configuration settings, continue with Validate the Configuration, page 38.

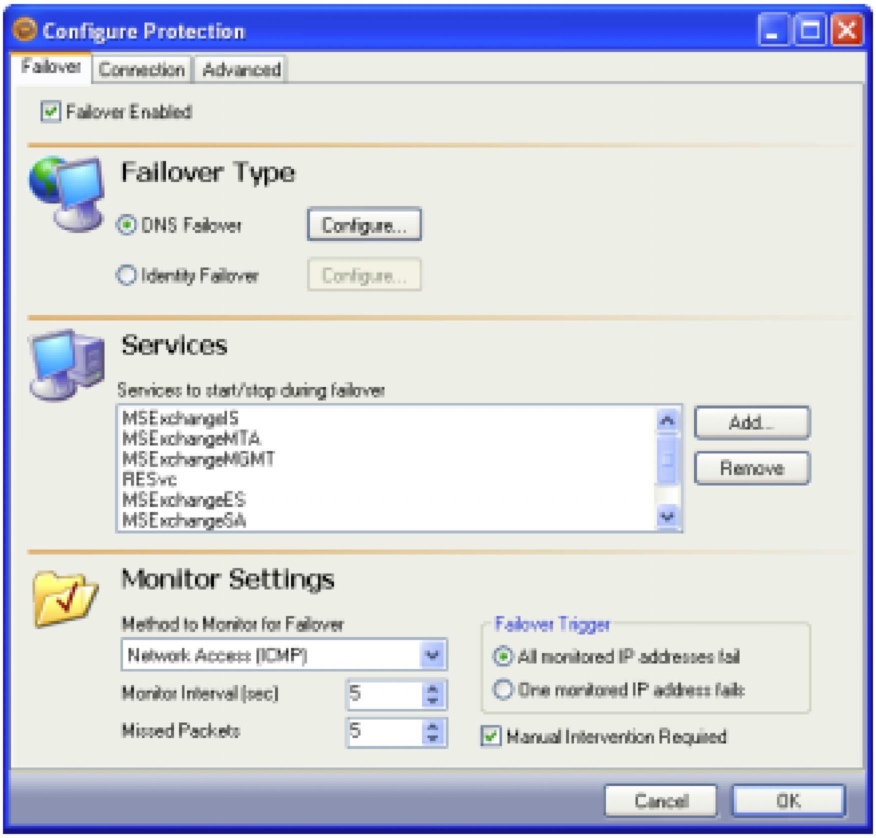
If you have already enabled protection for a connection and need to change the configuration parameters, you will first need to disable protection, as described in Disable protection, page 40.

To change the default configuration parameters, click **Configure** from the main Application Manager window, or select **Actions, Configure Protection** from the menu. The Configuration Protection window will appear.

The Configure Protection window has tabs for configuring failover, connection, and advanced settings. The following sections describe the options on each of these tabs.

Failover settings

The Failover tab includes options that will be applied during Exchange failover.



☑ Failover Enabled

● DNS Failover

○ Identity Failover

Services to start/stop during failover:

MSExchangeIS
MSExchangeMTA
MSExchangeMGMT
RESvc
MSExchangeES
MSExchangeSA

Method to Monitor for Failover: Network Access (ICMP)

Monitor Interval (sec): 5

Missed Packets: 5

Failover Trigger

● All monitored IP addresses fail

○ One monitored IP address fails

☑ Manual Intervention Required

Failover enabled

Select the **Failover enabled** option to enable or disable failover for the selected source/target pair.

Failover type

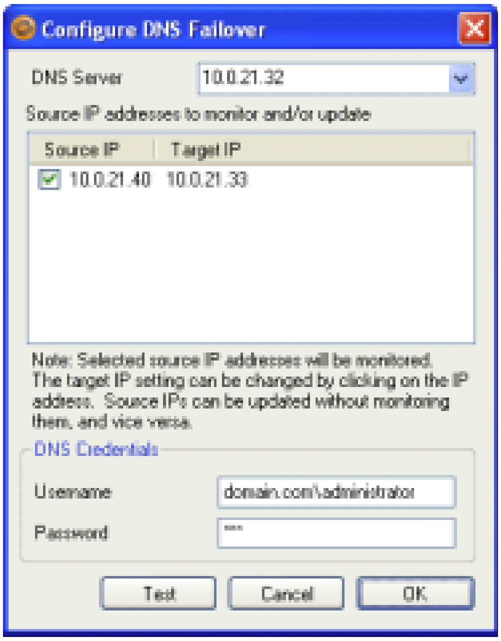
Failover Type indicates what name resolution method will be used to redirect users to the target Exchange server in the event of a source failure. By default, **DNS Failover** is selected.

DNS failover

DNS Failover is the recommended method for failover. Use this option if you want to failover by updating the DNS records associated with the source. This will modify all source server A, CNAME, MX, and PTR-type DNS resource records to point to the target.

In DNS Failover, the DNS records for the source server are modified to point to the target server’s IP address. This allows clients to resolve the source Exchange server name to the target server’s network name and IP address at failover time. DNS Failover eliminates duplicate server name and IP addresses on your network.

After you select the DNS Failover option, click **Configure**. The Configure DNS Failover window will appear.



DNS Server: 10.0.21.32

Source IP addresses to monitor and/or update

Source IP	Target IP
☑ 10.0.21.40	10.0.21.33

Note: Selected source IP addresses will be monitored. The target IP setting can be changed by clicking on the IP address. Source IPs can be updated without monitoring them, and vice versa.

DNS Credentials

Username: domain.com\administrator

Password: ***

The **DNS Server** field is automatically populated with the name of the source primary DNS server. You can select a different DNS server from the drop-down list.

Enter the following information for DNS failover:

- **Source IP**—Select the source IP address(es) to be monitored for failover.
- **Target IP**—Select the target IP address to be used when failover occurs.

  If one or more IP addresses are configured for the SMTP virtual server on the target, the first IP address will be the default target IP address for all source IP addresses.
- **Username**—Enter the user name that will be used to access/modify DNS records. The login account **MUST** be the DNS Admin for the domain in which the DNS server resides. For more information about permissions, see Appendix A: Recommended Credentials, page 48.

  You may enter a username for a different domain by entering a fully-qualified user name. The fully-qualified user name must be in the format **domain\username** or **username@domain**. If you enter a non-qualified name, the DNS domain will be used by default. The domain name is obtained from the DNS server name, provided that reverse lookup in DNS is enabled. For more information about enabling reverse lookup, refer to your Microsoft documentation.
- **Password**—Enter the password that will be used to access/modify DNS records.

After you have entered the information, click the **Test** button to validate that DNS failover is configured correctly and that the specified credentials are sufficient to update DNS. When the DNS configuration is complete, click **OK** to save your entries and return to the Configure Protection window.

NOTE:

- If you are running Windows Server 2000 on the primary DNS server hosting zones or domains that contain source and/or target resource records, you must have the DNS WMI Provider installed on that DNS server.
- If a hosts file entry for the source server exists on the client machine, errors may occur during a failover and failback.
- Reverse lookup in DNS should be enabled. For more information about enabling reverse lookup, refer to your Microsoft documentation.
- DNS registration for the private (devoted to Storage Mirroring) NIC IP should be disabled.
- To allow external email to be delivered to the target server when the source is unavailable, you should create an additional external MX record for the target server. The target MX record should have a lower priority than the source. Please refer to your router or firewall documentation for more information.
- If dynamic updates are enabled on a standard primary zone, the source server will be able to update its DNS records after failover. To prevent this, configure DNS to use an Active Directory-integrated zone.
- For more information about using the DNS Failover utility, access the `dfo.exe` help by typing **`dfo.exe /?`**.

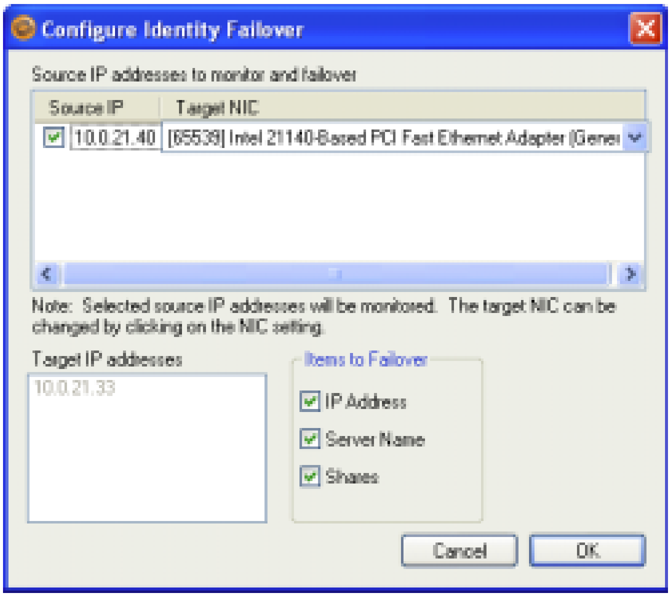
Identity failover

Select this option if you want to failover by transferring the source IP and name to the target. When using identity failover, it is possible that a name and/or IP address conflict can occur either during failover or when the original source server comes back online. To avoid this conflict, use **DNS Failover**.

In Identity Failover, the target's physical identity is modified to match the source during a failover. This includes the target adopting the source server's name, primary IP address, and drive shares. Identity failover may be required in the following situations:

- Access to the domain controller or DNS server is not available (for example, due to permissions) from the account that Storage Mirroring runs under on the source/target servers.
- If you determine that the time it takes to propagate the necessary DNS or Active Directory changes to the rest of your environment is not acceptable. The time needed to propagate these changes depends on your Active Directory Replication and DNS server settings.

After you select the Identity Failover option, click **Configure**. The Configure Identity Failover window will appear.



Source IP addresses to monitor and failover

Source IP	Target NIC
☑ 10.0.21.40	[65539] Intel 21140-Based PCI Fast Ethernet Adapter (Gener

Note: Selected source IP addresses will be monitored. The target NIC can be changed by clicking on the NIC setting.

Target IP addresses
10.0.21.33

Items to Failover
☑ IP Address
☑ Server Name
☑ Shares

Enter the following information for Identity failover:

- **Source IP**—Select the source IP address(es) to be monitored for failover.
- **Target NIC**—Select the target NIC to be used when failover occurs.
- **Target IP Addresses**—This area displays the IP address(es) of the selected target NIC.
- **IP Address**— *(Default = selected)* Select the **IP Address** checkbox if you want the specified source IP address to be added to the target when failover occurs.

  If you are in a WAN environment and choose **Identity Failover**, you should **NOT** failover the IP address.
- **Server Name**— *(Default = selected)* Select the **Server Name** checkbox if you want the source name to be added to the target when failover occurs.
- **Shares**— *(Default = selected)* Select the **Shares** checkbox if you want the source file shares to be added to the target when failover occurs.

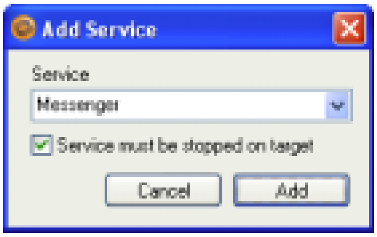
After the Identity failover configuration is complete, click **OK** to save your entries and return to the Configure Protection window.

Services

Storage Mirroring Application Manager will determine the appropriate Exchanges services to start/stop based on your operating system/Exchange configuration. You should only modify this selection if there are additional services that need to be started along with Exchange during the failover/failback process (such as BlackBerry®).

Modifying the default configuration for services may affect whether data can be successfully replicated. **Do not** modify the services to start/stop unless you are very familiar with Storage Mirroring and Exchange.

To add a service, click **Add**. In the Add Service window, select the Service name and whether the service must be stopped on the target for replication to occur properly. By default, this should be selected so that all target services are shut down during replication. Click **Add**.



Service
Messenger

☑ Service must be stopped on target

To remove a service, select the service, then click **Remove**. You can only remove services that you added manually using the Application Manager.

Resources (cluster only)

If you are using clustered Exchange servers, during configuration, you will select resources instead of services to bring online and offline during failover. The Resource selection works exactly like the service selection functionality.

Method to monitor for failover

The method to monitor for failover specifies the ping method to use when monitoring source IP addresses.

- **Network Access (ICMP)**—Storage Mirroring failover uses ICMP pings to determine if the source server is online. If a network device, such as a firewall or router, between the source and target is blocking ICMP traffic, failover monitors cannot be created or used.
- **Replication Service (UDP)**—The Storage Mirroring service on the target server sends a ping-like UDP request to the source Storage Mirroring service, which replies immediately to confirm it is running. This method is useful when ICMP is blocked on routers between the source and target.

Failover monitoring options

The amount of time before failover begins is calculated by multiplying the Failover Interval by the Missed Packets. For example, if the Failover Interval is set to 5 seconds and the Missed Packets setting is 5, a failover condition will be identified after 25 seconds of missed source activity.

- **Monitor Interval (sec)**—*(Default = 5)* How often the monitor checks the source machine availability.
- **Missed Packets (sec)**—*(Default = 5)* How many monitor replies can be missed before assuming the source machine has failed.

Failover trigger

If you are monitoring multiple IP addresses, select one of the failover trigger options:

- **All Monitored IP Addresses Fail**—Failover begins when all monitored IP addresses fail.
- **One Monitored IP Address Fails**—Failover begins when any of the monitored IP addresses fail.

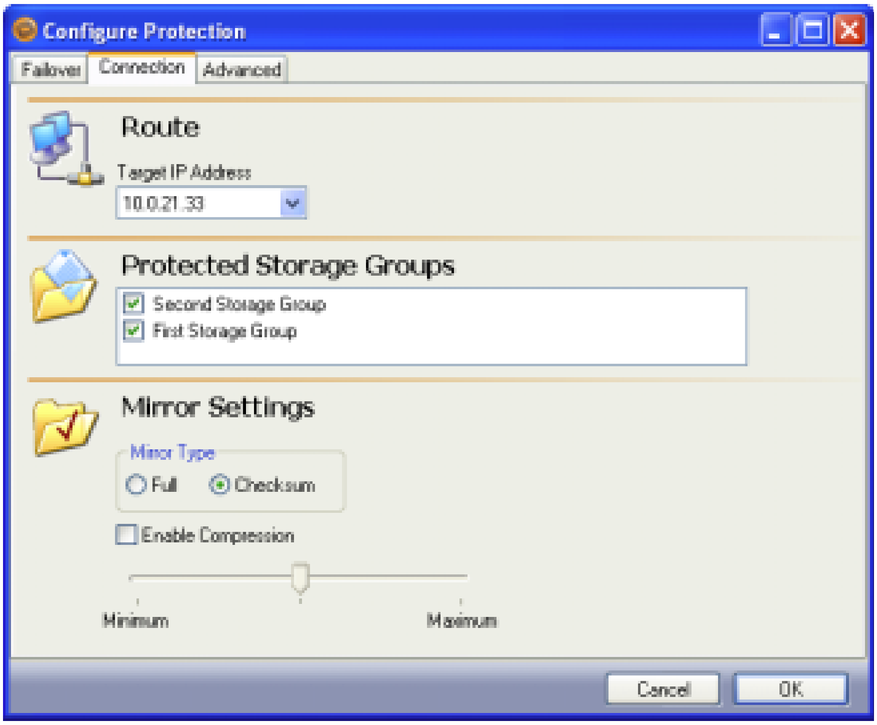
Manual intervention required

(Default = selected) Manual intervention allows you to control when failover occurs. When a failure occurs, a prompt appears and waits for you to initiate the failover process manually.

Disable **Manual Intervention Required** only if you want failover to occur immediately when a failure condition is met.

Connection settings

The Connection tab includes options that will be applied to the specified source/target connection.



Route

Target IP Address: 10.0.21.33

Protected Storage Groups

☑ Second Storage Group
☑ First Storage Group

Mirror Settings

Mirror Type: ○ Full ● Checksum

□ Enable Compression

Minimum — Maximum

Route

This setting identifies the Target IP address that the Storage Mirroring data will be transmitted through. You should only change this setting if you want to select a different route for Storage Mirroring traffic. On a machine with more than one NIC, this increases the flexibility of configuring Storage Mirroring activity. For example, you can separate regular network traffic and Storage Mirroring traffic on a machine. The default ports will be used.

Protected storage groups

Select the Exchange storage groups that you want to protect. By selecting individual storage groups to protect, you can reduce the amount of data being replicated and filter out storage groups that do not need to be protected or failed over. Only the users associated with the selected storage groups will be failed over. By default, all storage groups are selected for an Exchange source.

The replication set that the Application Manager generates will include the directories and files needed to protect the selected storage groups. It is recommended that you protect all storage groups.

NOTE: If you do not select all storage groups, you should make sure that other backups are available from which to recover the storage groups that are not failed over.

Mirror type

The following options specify what files you want sent from the source to the target during a mirror:

- **Full**—Copies all of the directories and files in the replication set to the target machine. If a mirror has already been completed, another full mirror will overwrite the data on the target.
- **Checksum**—*(Default)* This option compares the date, time, and size, and for those files that are different, a checksum calculation comparison is performed. A checksum calculation is a formula applied to blocks of data to determine if the binary make-up of the block is identical. If the checksums on the source and target machine are the same, the block is skipped. If the checksums on the source and target machine are not the same, the block on the source is sent to the target. With this option, the entire file is not overwritten; only the block that is received from the source is overwritten.

Enable compression

This setting enables compression of data that is transmitted from the source to the target. Significant improvements in bandwidth utilization have been seen in Wide Area Network (WAN) configurations, or in any case where network bandwidth is a constraint.

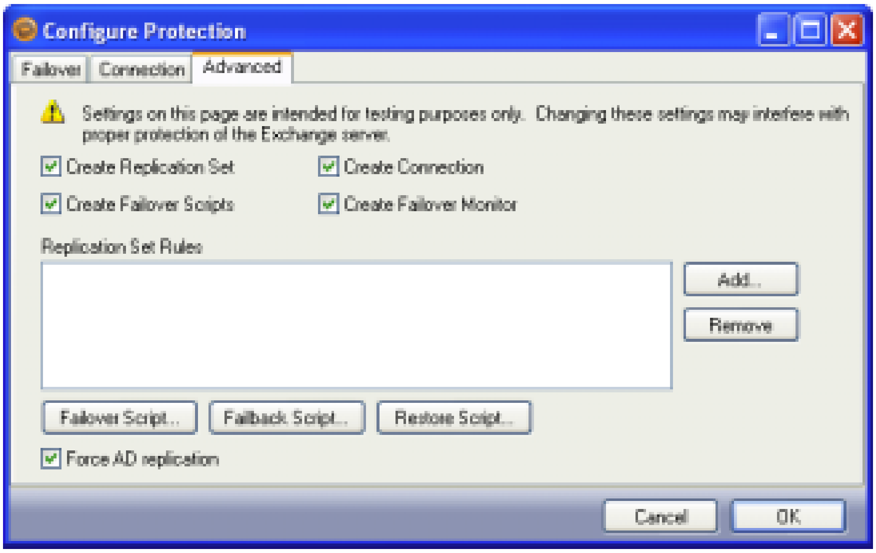
Compression may be used in Local Area Network (LAN) configurations, though it may not provide any significant network improvements.

You can specify compression for different source/target connections, but all connections to the same target will have the same compression settings.

By default, compression is disabled. To enable it, select **Enable Compression**, then set the level from minimum to maximum compression.

Advanced settings

The Advanced tab includes advanced configuration options.



Settings on this page are intended for testing purposes only. Changing these settings may interfere with proper protection of the Exchange server.

☑ Create Replication Set ☑ Create Connection

☑ Create Failover Scripts ☑ Create Failover Monitor

Replication Set Rules

☑ Force AD replication

Advanced settings

The following options allow you to control what functions Application Manager will perform during configuration. By default, Application Manager performs all of these functions. Individual functions should only be disabled for testing or debugging purposes.

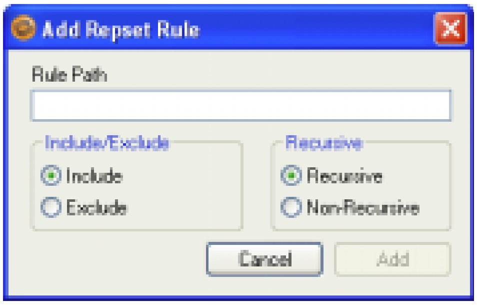
- **Create Replication Set**—*(Default = Selected)* Application Manager will automatically create a replication set that includes all of the necessary directories/files that must be protected for your specific configuration. This should only be disabled if you have customized your replication set and do not want to overwrite it.
- **Create Failover Scripts**—*(Default = Selected)* Application Manager will automatically generate the failover/failback scripts and copy them to the appropriate server. This should be disabled only if you have customized your script files and do not want them to be overwritten.
- **Create Connection**—*(Default = Selected)* Application Manager will create the appropriate connection between the source and target using the automatically-generated replication set. This should only be disabled if you would like to verify the replication set that is created by Application Manager prior to connection.
- **Create Failover Monitor**—*(Default = Selected)* Application Manager will create a failover monitor on the target to monitor the source for failure. This monitor will use the failover parameters specified during configuration, as well as the script files that have been created.

Replication set rules

A replication set defines what directories/files are to be protected by Storage Mirroring. By default, Application Manager selects all of the necessary directories/files to protect Exchange based on your source server configuration. These include all storage groups (system and log files), each database store (mailbox and public folder system and log files), Message Transfer Agent (MTA) files, and SMTP queues (pickup path and queuepath). By default, the Application Manager-generated replication set will be named `xdag01`.

You should only modify the replication set rules if there are additional directories/files specific to your configuration that must also be protected with Exchange. Modifying the default configuration for replication set rules may affect whether data can be successfully replicated. **Do not** modify the replication set unless you are very familiar with Storage Mirroring and Exchange.

To add a replication set rule, click **Add**. In the Add Repset Rule window, enter the rule path (the directory that you want to protect or exclude), select whether to include/exclude the path, and whether the directory should be recursive or non-recursive. Click **Add**. You will need to manually verify that the rule path is correct since the Application Manager does not validate rule paths,



To remove a rule, select the rule, then click **Remove**. You can only remove rules that you added manually through the Application Manager. Rules that are automatically added by Application Manager cannot be removed or changed through the Application Manager interface.

NOTE: If you want to protect the Badmail folder, you will need to manually add it to the replication set.

Failover/failback scripts

Scripts are executed at different points during the failover/failback process to perform the actions necessary to make Exchange available on the appropriate server. Scripts perform steps such as starting/stopping services, modifying mailbox values in Active Directory to point users to the appropriate server, and modifying DNS entries on the DNS server to point users to the appropriate server.

Editing scripts is an advanced feature. **Do not** edit scripts unless you fully understand what each command is doing.

Three scripts are automatically generated by Application Manager during configuration. The scripts are copied to the Storage Mirroring installation directory on the specified server using the administrative share for that server's drive.

- **Failover Script**—A post-failover script (`tempPostFailover.txt`) is executed after the core failover processes have completed on the target server. The primary functions of the post-failover script are to start the Exchange services on the target and to modify DNS and Active Directory entries as necessary.
- **Failback Script**—A pre-failback script (`tempPreFailback.txt`) is executed before failback processing occurs on the target server. The primary functions of this script are to stop Exchange services on the target and to move DNS and Active Directory entries as necessary.
- **Restore Script**—A post-restore script (`tempPostRestore.txt`) is not executed automatically, though it is provided on the source to perform actions that are generally required after data has been restored from the target to source after a failover/failback. The primary function of this script is to restart Exchange services on the source server and rehome the public folders hosted on the source server.

By default, Application Manager generates all the required scripts for you automatically based on your system configuration. You can also edit the scripts to add, modify, or delete specific commands. To edit a script, click on the button for the script you want to update and the script file will be displayed using your machine's default editor. Enter your changes, then save the script file. Any change you make to the script in the editor will be copied to the appropriate server when configuration changes are accepted, thus overwriting any changes that have been made outside the Application Manager.

The scripts can be overwritten by certain operations during setup. For example, any changes to configuration options done in the Application Manager will overwrite previous script changes. **If you want to make permanent changes to a script**, you must modify the appropriate `.txt` file within the Exchange Failover installation directory. If there is more than one client machine that will be configuring failover, the change must be made to all the appropriate `.txt` files (`post_failover.txt`, `post_restore.txt`, and `pre_failback.txt`).

Before running Application Manager multiple times (for example, when re-enabling protection after a failover/failback), save a copy of your post-restore and pre-failback batch files. After Application Manager executes, replace the default script file(s) with the customized file(s) that you saved.

Force AD replication

(Default = selected) When selected, replication is initiated from the domain controller with which the source or target server communicates. This will be done each time the Exchange Failover utility (exchfailover.exe) is executed from within the failover/failback scripts. For more information about using the Exchange Failover utility, see Appendix F: Using the Exchange Failover (EFO) Utility, page 73.

Disable **Force AD Replication** if you do not want Active Directory changes to be replicated.

Saving configuration changes

After you have changed the configuration parameters, click **OK** to apply the settings. If you click **Cancel**, any changes you have made will be discarded and the previous configuration parameters will be used.

When you have finished configuring the optional protection options, continue with Validate the Configuration, page 38.

NOTE: If you close the Storage Mirroring Application Manager prior to enabling protection, your changes will not be saved. You **must** enable protection in order to save your configuration settings for a source/target pair.

Protecting a SQL Server

SQL configuration workflow

To configure protection for your SQL servers using Application Manager, you will complete the following steps:

1. Install Storage Mirroring on the source and target Exchange servers. See the Storage Mirroring *Getting Started* guide for more information.
2. Install the Storage Mirroring Application Manager, page 10
3. Select a task, page 25
4. Select a domain, page 26
5. Select source and target servers, page 26
6. (Optional) Configure protection settings, page 28
7. Validate the Configuration, page 38

To protect your SQL server, you will complete the following steps:

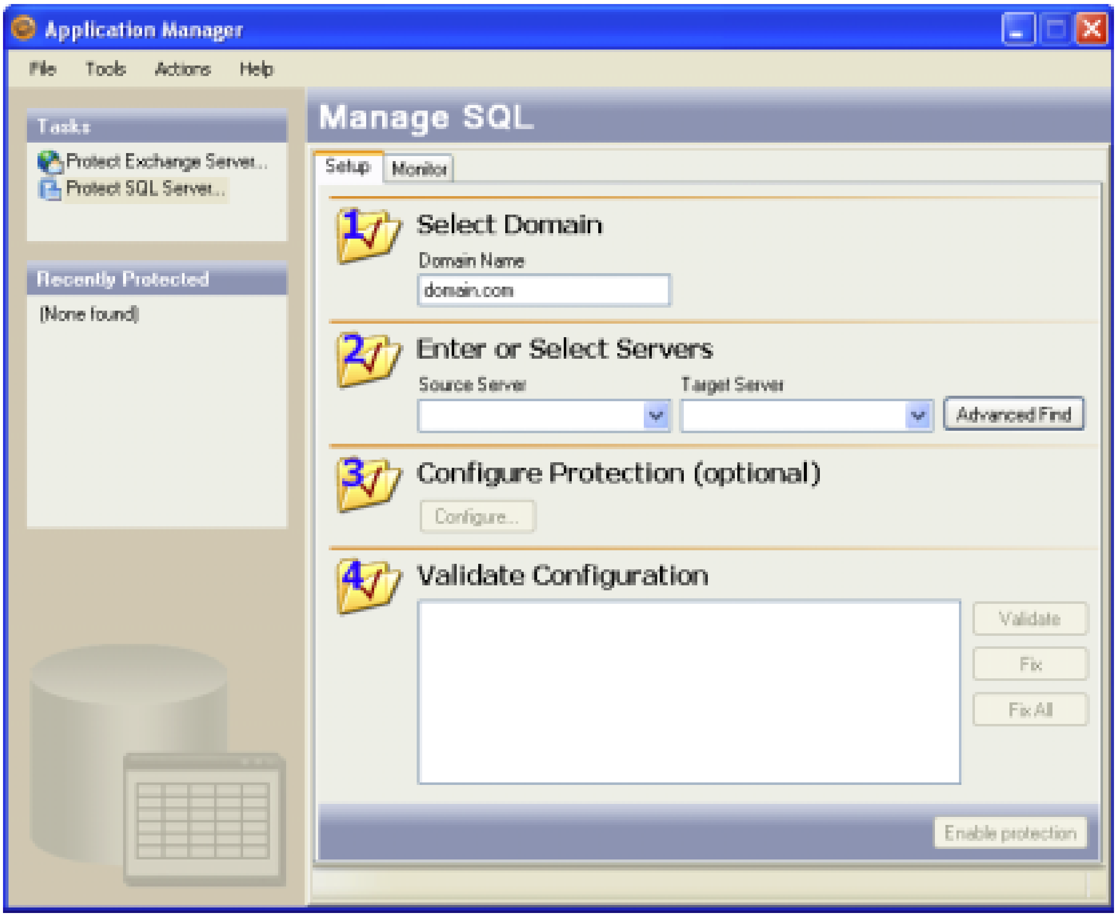
1. Enable protection, page 39
2. Monitor protection status, page 40

In the event of a failure, you will need to perform some additional tasks. These tasks are described in Failover, Failback, and Restoration, page 43.

Select a task

To protect a SQL server, either open the Application Manager for Exchange (**Start, Programs, Storage Mirroring, Application Manager, SQL Manager**), or from the Tasks area on the left pane, select **Protect SQL Server**. The Manage SQL page will appear in the right pane. Make sure that the Setup tab is in view.

If you have previously configured protection for a source/target pair, the Manage SQL page will be populated with information about the protected pair.



Domain Name: domain.com

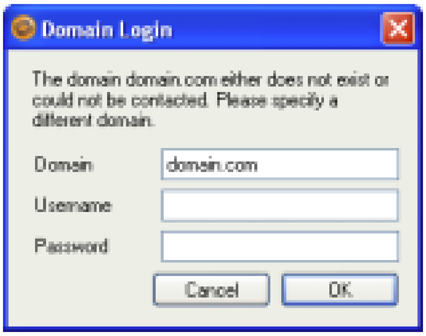
Select a domain

The **Domain Name** on the main window will be populated automatically with the domain where the Application Manager client resides.

If you want to change the domain, type in a domain name for a trusted domain that the Application Manager client can connect to, then press Tab or click on another field. If the domain you entered doesn't exist or you do not have the credentials to modify Active Directory for the new domain, the Domain Login window will appear. You will be prompted to enter the domain name, user name, and password to use for logging in to the domain.

The user account should have *administrator* permissions. For more information about permissions, see Appendix A: Recommended Credentials, page 48.

You may enter a username for a different domain by entering a fully-qualified user name. The fully-qualified user name must be in the format **domain\username** or **username@domain**. If you enter a non-qualified name, the default domain will be used.



The domain domain.com either does not exist or could not be contacted. Please specify a different domain.

Domain: domain.com

Username:

Password:

Select source and target servers

You can either type the source and target server names into the **Source Server** and **Target Server** lists, or you can click the **Advanced Find** button and add the servers. For more information, see Add or manage servers, page 27.

If you select a source/target pair for which you have previously enabled and disabled protection, you may use the existing configuration settings (provided that the source/target connection is not currently active, in which case the existing settings will always be used). When you select **Configure** or **Validate**, a prompt will appear, asking if you want to re-use the previous configuration information. Click **Yes** to re-use the previous information, or click **No** to revert to the Application Manager default settings.

NOTE: If the IP address(es) for the source or target server have changed since you originally configured protection (for example, if you configure the source or target in a staging area and then send it to a production location), you must re-configure the protection settings. When you are prompted to re-use the previous protection configuration, click **No**, then click the **Configure Protection** button.

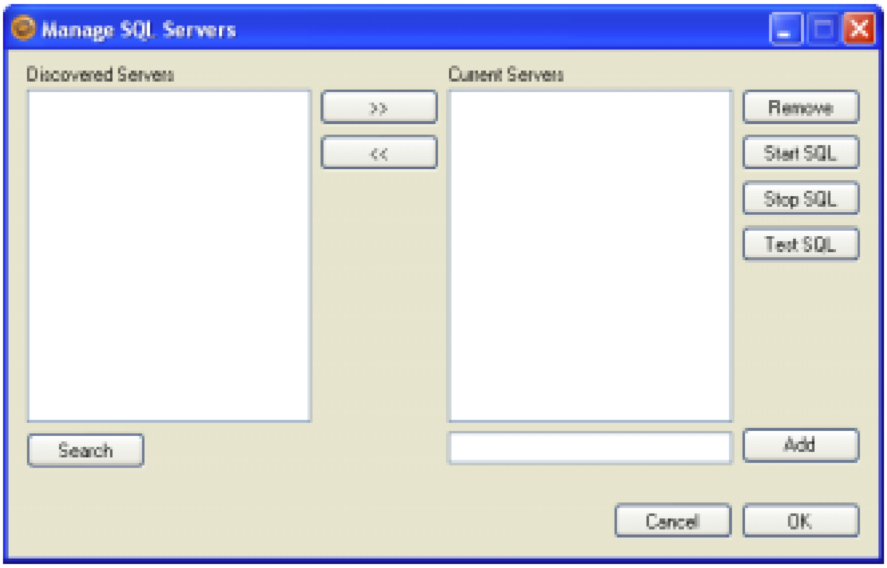
1. In the **Source Server** field, select the SQL server that you want to protect. If this is your first time to log in to the selected server, you will be prompted to enter server login information. For more information about logging in to servers, see Enter server login information, page 27.
2. In the **Target Server** field, select the backup SQL server that will protect the source server in the event of a failure.

Notice that after you select a server to protect, the Protection Status changes to “Unprotected”.

NOTE: If you select a target that is monitoring a connection that has met a failover condition and requires manual intervention, a prompt will appear, asking if you want to initiate failover.

Add or manage servers

If the servers you need do not appear, click the **Advanced Find** button, or select **Actions, Manage SQL Servers**. The Manage SQL Servers window will appear.



To discover all servers in the domain, click the **Search** button. The Discovered Servers list will be populated with all servers that the Application Manager can discover that reside in the domain.

To directly add a server to the drop-down list on the Manage SQL main page, select the server in the **Discovered Servers** list, then use the **>>** button to move it into the **Current Servers** list.

To add a non-discovered server to the Current Servers list, enter the server name in the field next to the Add button, then click the **Add** button.

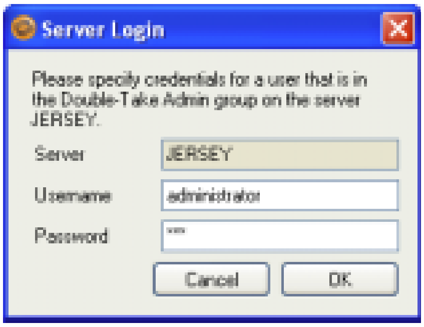
After a server has been added to the Current Servers list, you can manage that server. Select the server, then select one of the following options:

- **Remove**—Click the **Remove** button to remove the selected server from the drop-down list on the Manage SQL main page.
- **Start SQL**—Click the **Start SQL** button to start SQL services on the selected server. The SQL services must be started in order for the Application Manager to verify that SQL is installed on the server and to query the server's information.
- **Stop SQL**—Click the **Stop SQL** button to stop SQL services on the selected server.
- **Test SQL**—Click the **Test SQL** button to determine if SQL is installed and accessible for the selected server.

When you have finished adding, managing, or testing servers, click **OK** to save your changes, or **Cancel** to return to the Manage SQL main page without saving.

Enter server login information

After you select a server for the first time, you will be prompted to enter a user name and password to use for logging in to the selected server. The login account **MUST** be a member of the Storage Mirroring Admin local security group for the selected server. For more information about permissions, see Appendix A: Recommended Credentials, page 48.



Please specify credentials for a user that is in the Double-Take Admin group on the server JERSEY.

Server: JERSEY

Username: administrator

Password: ***

You may enter a username for a different domain by entering a fully-qualified user name. The fully-qualified user name must be in the format **domain\username** or **username@domain**. If you enter a non-qualified name, the DNS domain will be used.

The Application Manager will attempt to use the same user name and password the next time you select a server.

Configure protection settings

If you do not need to change the configuration settings, continue with Validate the Configuration, page 38.

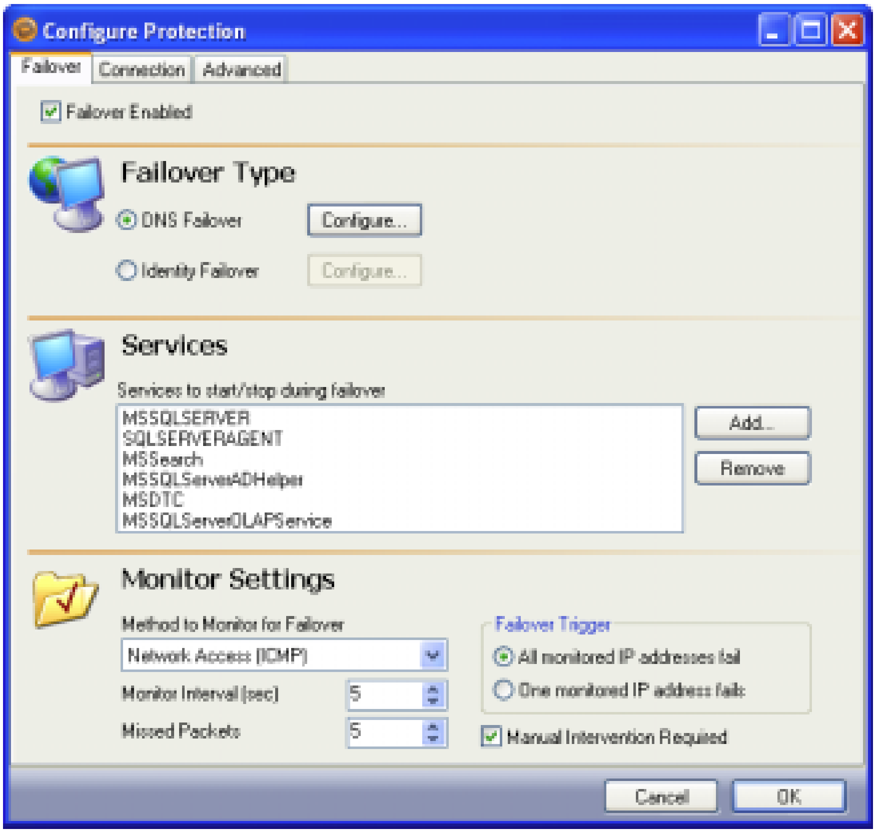
If you have already enabled protection for a connection and need to change the configuration parameters, you will first need to disable protection, as described in Disable protection, page 40.

To change the default configuration parameters, click **Configure** from the main Application Manager window, or select **Actions, Configure Protection** from the menu. The Configuration Protection window will appear.

The Configure Protection window has tabs for configuring failover, connection, and advanced settings. The following sections describe the options on each of these tabs.

Failover settings

The Failover tab includes options that will be applied during SQL failover.



☑ Failover Enabled

● DNS Failover

○ Identity Failover

Services to start/stop during failover

MSSQLSERVER
SQLSERVERAGENT
MSSearch
MSSQLServerADHelper
MSDTC
MSSQLServerOLAPService

Method to Monitor for Failover: Network Access (ICMP)

Monitor Interval (sec): 5

Missed Packets: 5

Failover Trigger
● All monitored IP addresses fail
○ One monitored IP address fails

☑ Manual Intervention Required

Failover enabled

Select the Failover Enabled option to enable or disable failover for the selected source/target pair.

Failover type

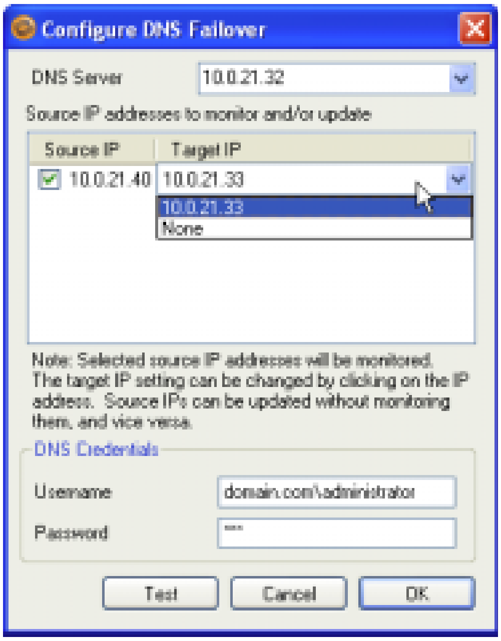
Failover Type indicates what name resolution method will be used to redirect users to the target SQL server in the event of a source failure. By default, **DNS Failover** is selected.

DNS failover

DNS Failover is the recommended method for failover. Use this option if you want to failover by updating the DNS records associated with the source. This will modify all source server A, CNAME, MX, and PTR-type DNS resource records to point to the target.

In DNS Failover, the DNS records for the source server are modified to point to the target server’s IP address. This allows clients to resolve the source SQL server name to the target server’s network name and IP address at failover time. DNS Failover reduces the risk of duplicate server name and IP addresses on your network.

After you select the DNS Failover option, click **Configure**. The Configure DNS Failover window will appear.



DNS Server: 10.0.21.32

Source IP addresses to monitor and/or update

Source IP	Target IP
☑ 10.0.21.40	10.0.21.33 10.0.21.33 None

Note: Selected source IP addresses will be monitored. The target IP setting can be changed by clicking on the IP address. Source IPs can be updated without monitoring them, and vice versa.

Username: domain.com\administrator

Password: ***

The **DNS Server** field is automatically populated with the name of the source primary DNS server. You can select a different DNS server from the drop-down list.

Enter the following information for DNS failover:

- **Source IP**—Select the source IP address(es) to be monitored for failover.
- **Target IP**—Select the target IP address to be used when failover occurs.
- **Username**—Enter the user name that will be used to access/modify DNS records. The login account **MUST** be the DNS Admin for the domain in which the DNS server resides. For more information about permissions, see Appendix A: Recommended Credentials, page 48.

  You may enter a username for a different domain by entering a fully-qualified user name. The fully-qualified user name must be in the format **domain\username** or **username@domain**. If you enter a non-qualified name, the DNS domain will be used by default. The domain name is obtained from the DNS server name, provided that reverse lookup in DNS is enabled. For more information about enabling reverse lookup, refer to your Microsoft documentation.
- **Password**—Enter the password that will be used to access/modify DNS records.

After you have entered the information, click the **Test** button to validate that DNS failover is configured correctly and that the specified credentials are sufficient to update DNS. When the DNS configuration is complete, click **OK** to save your entries and return to the Configure Protection window.

NOTE:

- If you are running Windows Server 2000 on the primary DNS server hosting zones or domains that contain source and/or target resource records, you must have the DNS WMI Provider installed on that DNS server.
- If a hosts file entry for the source server exists on the client machine, errors may occur during a failover and failback.
- Reverse lookup in DNS should be enabled. For more information about enabling reverse lookup, refer to your Microsoft documentation.
- DNS registration for the private (devoted to Storage Mirroring) NIC IP should be disabled.
- If dynamic updates are enabled on a standard primary zone, the source server will be able to update its DNS records after failover. To prevent this, configure DNS to use an Active Directory-integrated zone.
- For more information about using the DNS Failover utility, access the `dfo.exe` help by typing **`dfo.exe /?`**.

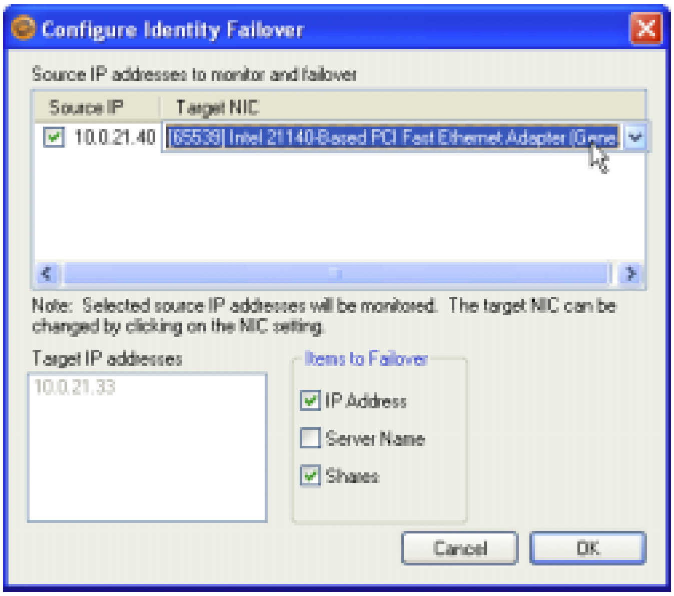
Identity failover

Select this option if you want to failover by transferring the source IP and name to the target. When using identity failover, it is possible that a name and/or IP address conflict can occur either during failover or when the original source server comes back online. To avoid this conflict, use **DNS Failover**.

In Identity Failover, the target will adopt the source server's name, primary IP address, and drive during a failover. Identity failover may be required in the following situations:

- Access to the domain controller or DNS server is not available (for example, due to permissions) from the account that Storage Mirroring runs under on the source/target servers.
- If you determine that the time it takes to propagate the necessary DNS or Active Directory changes to the rest of your environment is not acceptable. The time needed to propagate these changes depends on your Active Directory Replication and DNS server settings.
- If you want to fail over shares from the source to the target.

After you select the Identity Failover option, click **Configure**. The Configure Identity Failover window will appear.



Source IP addresses to monitor and failover

Source IP	Target NIC
☑ 10.0.21.40	[65539] Intel 21140-Based PCI Fast Ethernet Adapter (Gene

Note: Selected source IP addresses will be monitored. The target NIC can be changed by clicking on the NIC setting.

Target IP addresses: 10.0.21.33

Items to Failover

☑ IP Address

□ Server Name

☑ Shares

Enter the following information for Identity failover:

- **Source IP**—Select the source IP address(es) to be monitored for failover.
- **Target NIC**—Select the target NIC to be used when failover occurs.
- **Target IP Addresses**—This area displays the IP address(es) of the selected target NIC.
- **IP Address**— *(Default = selected)* Select the **IP Address** checkbox if you want the specified source IP address to be added to the target when failover occurs.

  If you are in a WAN environment and choose **Identity Failover**, you should **NOT** failover the IP address.
- **Server Name**— *(Default = selected)* Select the **Server Name** checkbox if you want the source name to be added to the target when failover occurs.
- **Shares**— *(Default = selected)* Select the **Shares** checkbox if you want the source file shares to be added to the target when failover occurs.

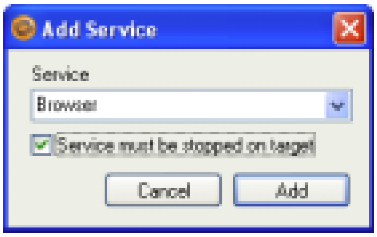
After the Identity failover configuration is complete, click **OK** to save your entries and return to the Configure Protection window.

Services

Storage Mirroring Application Manager will determine the appropriate SQL services to start/stop based on your operating system/SQL configuration. You should only modify this selection if there are additional services that need to be started along with SQL during the failover/failback process.

Modifying the default configuration for services may affect whether data can be successfully replicated. **Do not** modify the services to start/stop unless you are very familiar with Storage Mirroring and SQL.

To add a service, click **Add**. In the Add Service window, select the Service name and whether the service must be stopped on the target for replication to occur properly. By default, this should be selected so that all target services are shut down during replication. Click **Add**.



To remove a service, select the service, then click **Remove**. You can only remove services that you added manually using the Application Manager.

Method to monitor for failover

The method to monitor for failover specifies the ping method to use when monitoring source IP addresses.

- **Network Access (ICMP)**—Storage Mirroring failover uses ICMP pings to determine if the source server is online. If a network device, such as a firewall or router, between the source and target is blocking ICMP traffic, failover monitors cannot be created or used.
- **Replication Service (UDP)**—**Replication Service (UDP)**—The Storage Mirroring service on the target server sends a ping-like UDP request to the source Storage Mirroring service, which replies immediately to confirm it is running. This method is useful when ICMP is blocked on routers between the source and target.

Failover monitoring options

The amount of time before failover begins is calculated by multiplying the Failover Interval by the Missed Packets. For example, if the Failover Interval is set to 5 seconds and the Missed Packets setting is 5, a failover condition will be identified after 25 seconds of missed source activity.

- **Monitor Interval (sec)**—*(Default = 5)* How often the monitor checks the source machine availability.
- **Missed Packets (sec)**—*(Default = 5)* How many monitor replies can be missed before assuming the source machine has failed.

Failover trigger

If you are monitoring multiple IP addresses, select one of the failover trigger options:

- **All Monitored IP Addresses Fail**—Failover begins when all monitored IP addresses fail.
- **One Monitored IP Address Fails**—Failover begins when any of the monitored IP addresses fail.

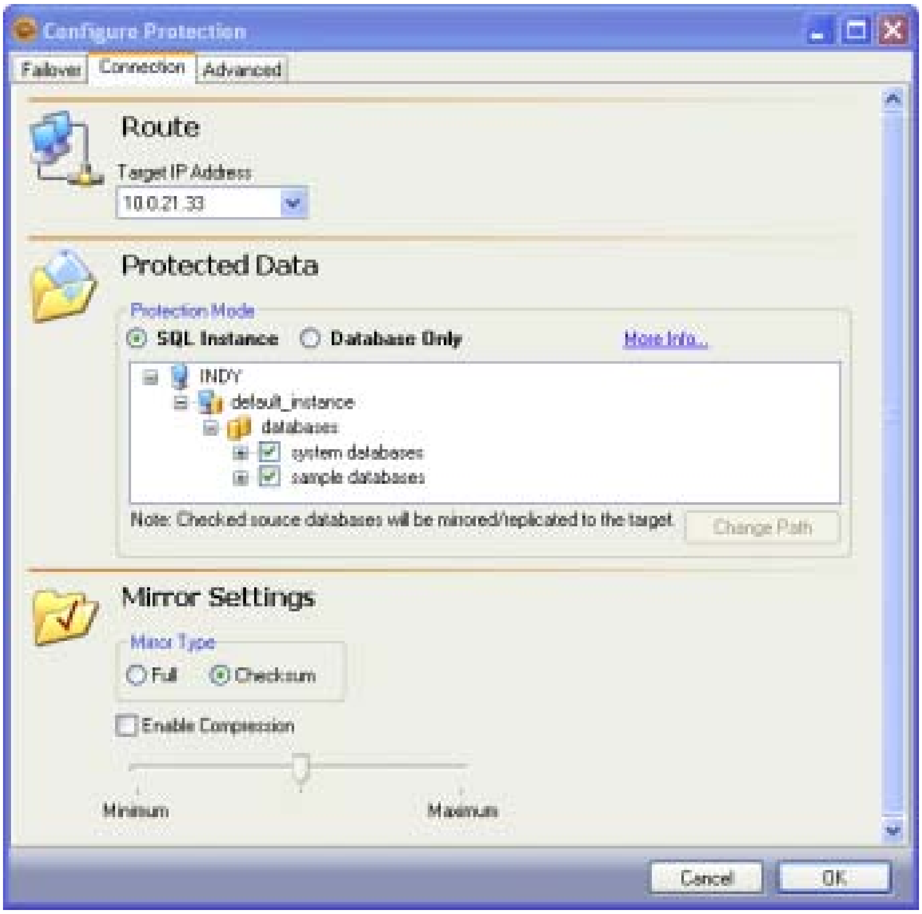
Manual intervention required

(Default = selected) Manual intervention allows you to control when failover occurs. When a failure occurs, a prompt appears and waits for you to initiate the failover process manually.

Disable **Manual Intervention Required** only if you want failover to occur immediately when a failure condition is met.

Connection settings

The Connection tab includes options that will be applied to the specified source/target connection.



Route

Target IP Address: 10.0.21.33

Protected Data

Protection Mode

● SQL Instance ○ Database Only More Info...

- INDY
  - default_instance
    - databases
      - ☑ system databases
      - ☑ sample databases

Note: Checked source databases will be mirrored/replicated to the target. Change Path

Mirror Settings

Mirror Type

○ Full ● Checksum

□ Enable Compression

Minimum Maximum

Route

This setting identifies the Target IP address that the Storage Mirroring data will be transmitted through. You should only change this setting if you want to select a different route for Storage Mirroring traffic. On a machine with more than one NIC, this increases the flexibility of configuring Storage Mirroring activity. For example, you can separate regular network traffic and Storage Mirroring traffic on a machine. The default ports will be used.

Protection mode

For SQL, you can select one of the following protection modes:

- **SQL Instance**—(default) Select **SQL Instance** protection mode to replicate all of the SQL program and data files (except the \bin directory) to the target SQL server. This will allow the clients to access your production SQL Server data and functionality on the target in the event of a failure.

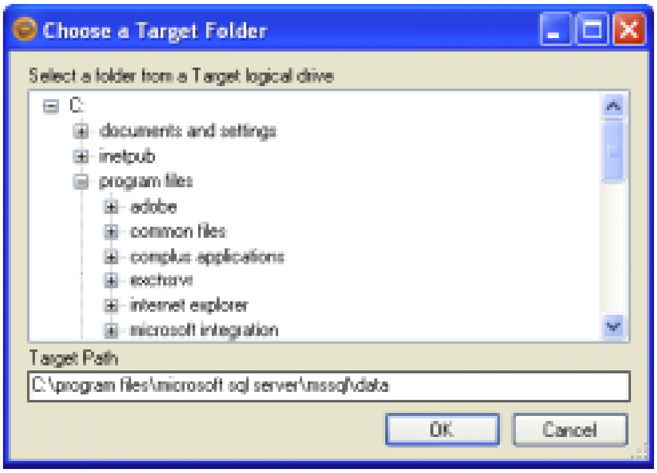
  SQL Instance protection mode requires that the source and target servers both have the exact same version of SQL (major and minor versions) as well as similar logical drive structures (the target must have at least the same logical drives as the source where SQL program and data files are stored). Certain user databases can be de-selected, but the System databases (except for `tempdb`) are required.

- **Database Only**—(advanced users only) Select **Database Only** protection mode to replicate *only* the `.mdf`, `.ldf`, and `.ndf` files to the target server. The selected database(s) will be attached to the target SQL Server upon failover, allowing clients to access the underlying data.

  During the configuration and validation process, you will have the opportunity to transfer user logins and permissions (both server and database-level) and certain SQL Server registry and configuration settings to the target server. This will allow users to access the data associated with the selected database(s), but no other server-level functionality will be transferred to the target server (including but not limited to Job Server configuration, Full-Text service configuration, SQL Replication configuration, linked servers, remote servers, backup devices).

NOTE: When using Database Only mode, any SQL Server replication configured on the protected databases must be configured by the administrator on the target after failover.

If you select Database Only protection mode, you can select a non-system database and map it to a unique path on the target. Select the database you want to re-map, then click the **Change Path** button. The Choose a Target Folder window will appear:



Target Path: C:\program files\microsoft sql server\mssql\data

Enter the desired path in the **Target Path** field, then click **OK**.

Mirror type

The following options specify what files you want sent from the source to the target during a mirror:

- **Full**—Copies all of the directories and files in the replication set to the target machine. If a mirror has already been completed, another full mirror will overwrite the data on the target.
- **Checksum**—*(Default)* This option compares the date, time, and size, and for those files that are different, a checksum calculation comparison is performed. A checksum calculation is a formula applied to blocks of data to determine if the binary make-up of the block is identical. If the checksums on the source and target machine are the same, the block is skipped. If the checksums on the source and target machine are not the same, the block on the source is sent to the target. With this option, the entire file is not overwritten; only the block that is received from the source is overwritten.

Enable compression

This setting enables compression of data that is transmitted from the source to the target. Significant improvements in bandwidth utilization have been seen in Wide Area Network (WAN) configurations, or in any case where network bandwidth is a constraint.

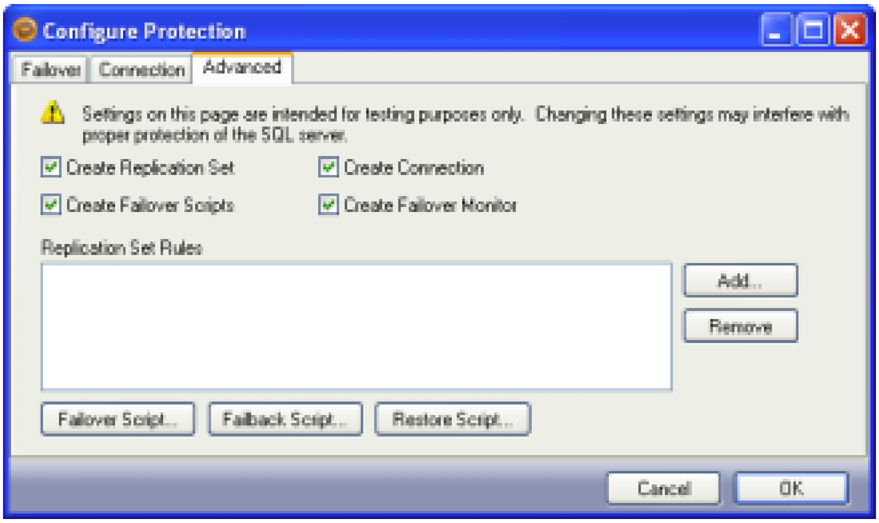
Compression may be used in Local Area Network (LAN) configurations, though it may not provide any significant network improvements.

You can specify compression for different source/target connections, but all connections to the same target will have the same compression settings.

By default, compression is disabled. To enable it, select **Enable Compression**, then set the level from minimum to maximum compression.

Advanced settings

The Advanced tab includes advanced configuration options.



Settings on this page are intended for testing purposes only. Changing these settings may interfere with proper protection of the SQL server.

☑ Create Replication Set ☑ Create Connection

☑ Create Failover Scripts ☑ Create Failover Monitor

Advanced settings

The following options allow you to control what functions Application Manager will perform during configuration. By default, Application Manager performs all of these functions. Individual functions should only be disabled for testing or debugging purposes.

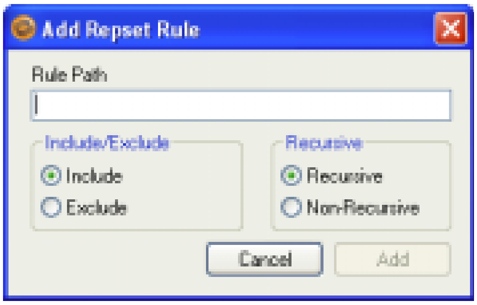
- **Create Replication Set**—*(Default = Selected)* Application Manager will automatically create a replication set that includes all of the necessary directories/files that must be protected for your specific configuration. This should only be disabled if you have customized your replication set and do not want to overwrite it.
- **Create Failover Scripts**—*(Default = Selected)* Application Manager will automatically generate the failover/failback scripts and copy them to the appropriate server. This should be disabled only if you have customized your script files and do not want them to be overwritten.
- **Create Connection**—*(Default = Selected)* Application Manager will create the appropriate connection between the source and target using the automatically-generated replication set. This should only be disabled if you would like to verify the replication set that is created by Application Manager prior to connection.
- **Create Failover Monitor**—*(Default = Selected)* Application Manager will create a failover monitor on the target to monitor the source for failure. This monitor will use the failover parameters specified during configuration, as well as the script files that have been created.

Replication set rules

A replication set defines what directories/files are to be protected by Storage Mirroring. By default, Application Manager selects all of the necessary directories/files to protect SQL based on your source server configuration. These include the SQL application data and transaction logs, tempdb files, and SQL error logs. By default, the Application Manager-generated replication set will be named `sqldag01`.

You should only modify the replication set rules if there are additional directories/files specific to your configuration that must also be protected with SQL. Modifying the default configuration for replication set rules may affect whether data can be successfully replicated. **Do not** modify the replication set unless you are very familiar with Storage Mirroring and SQL.

To add a replication set rule, click **Add**. In the Add Repset Rule window, enter the rule path (the directory that you want to protect or exclude), select whether to include/exclude the path, and whether the directory should be recursive or non-recursive. Click **Add**. You will need to manually verify that the rule path is correct since the Application Manager does not validate rule paths,



To remove a rule, select the rule, then click **Remove**. You can only remove rules that you added manually through the Application Manager. Rules that are automatically added by Application Manager cannot be removed or changed through the Application Manager interface.

Failover/failback scripts

Scripts are executed at different points during the failover/failback process to perform the actions necessary to make SQL available on the appropriate server. Scripts perform steps such as starting/stopping services, modifying mailbox values in Active Directory to point users to the appropriate server, and modifying DNS entries on the DNS server to point users to the appropriate server.

Editing scripts is an advanced feature. **Do not** edit scripts unless you fully understand what each command is doing.

Three scripts are automatically generated by Application Manager during configuration. The scripts are copied to the Storage Mirroring installation directory on the specified server using the administrative share for that server's drive.

- **Failover Script**—A post-failover script (`tempPostFailover.txt`) is executed after the core failover processes have completed on the target server. The primary functions of the post-failover script are to start the SQL services on the target and to modify DNS and Active Directory entries as necessary.
- **Failback Script**—A pre-failback script (`tempPreFailback.txt`) is executed before failback processing occurs on the target server. The primary functions of this script are to stop SQL services on the target and to move DNS and Active Directory entries as necessary.
- **Restore Script**—A post-restore script (`tempPostRestore.txt`) is not executed automatically, though it is provided on the source to perform actions that are generally required after data has been restored from the target to source after a failover/failback. The primary function of this script is to restart SQL services on the source server and rehome the public folders hosted on the source server.

By default, Application Manager generates all the required scripts for you automatically based on your system configuration. You can also edit the scripts to add, modify, or delete specific commands. To edit a script, click on the button for the script you want to update and the script file will be displayed using your machine's default editor. Enter your changes, then save the script file. Any change you make to the script in the editor will be copied to the appropriate server when configuration changes are accepted, thus overwriting any changes that have been made outside the Application Manager.

The scripts can be overwritten by certain operations during setup. For example, any changes to configuration options done in the Application Manager will overwrite previous script changes. **If you want to make permanent changes to a script**, you must modify the appropriate `.txt` file within the SQL Failover installation directory. If there is more than one client machine that will be configuring failover, the change must be made to all the appropriate `.txt` files (`post_failover_sql.txt`, `post_restore_sql.txt`, and `pre_failback_sql.txt`).

Before running Application Manager multiple times (for example, when re-enabling protection after a failover/failback), save a copy of your post-restore and pre-failback batch files. After Application Manager executes, replace the default script file(s) with the customized file(s) that you saved.

Saving configuration changes

After you have changed the configuration parameters, click **OK** to apply the settings. If you click **Cancel**, any changes you have made will be discarded and the previous configuration parameters will be used.

When you have finished configuring the optional protection options, continue with the next section, Validate the Configuration.

NOTE: If you close the Storage Mirroring Application Manager prior to enabling protection, your changes will not be saved. You **must** enable protection in order to save your configuration settings for a source/target pair.

Validate the Configuration

Click **Validate**, or select **Actions, Validate**, to ensure that the source and target servers are configured correctly for failover. A description of the validation activity being performed is displayed in the status bar at the bottom of the Application Manager window, along with status progress indicator. When validation completes, the status progress indicator is removed.

- If you are using DNS Failover and did not enter DNS credentials on the Configure Protection window, you will be prompted to enter a user name and password for accessing/modifying DNS records.
- If the configuration is good, a green checkmark icon will appear next to a validation message that states that the servers are configured correctly. Continue with the next section, Enable protection.
- If the validation detects potential configuration issues, an icon will appear next to the message(s). The following table identifies the icons and the validation conditions that they represent. Double-click on a message to view details concerning the issue. On the Validation Details window, review the additional information, and, if available, click **Fix** and Application Manager will attempt to resolve the issue. If you would rather address the issue manually, click **Cancel**. After correcting any issues, click **Validate** again to verify the change was made. For more information about the error messages, see Appendix C: Exchange Validation Messages, page 52 or Appendix D: SQL Validation Messages, page 61.

Icon	Validation Status
✓	Good
?	Unknown
✖	Error, Fixable—If not fixed, failover cannot occur. Can be fixed by Application Manager.
✖	Error, Not Fixable—If not fixed, failover cannot occur. Must be fixed manually.
⚠	Warning, Fixable—The Application Manager detected an issue that should be addressed prior to failover. Can be fixed by Application Manager.
⚠	Warning, Not Fixable—The Application Manager detected an issue that should be addressed prior to failover. Must be fixed manually.

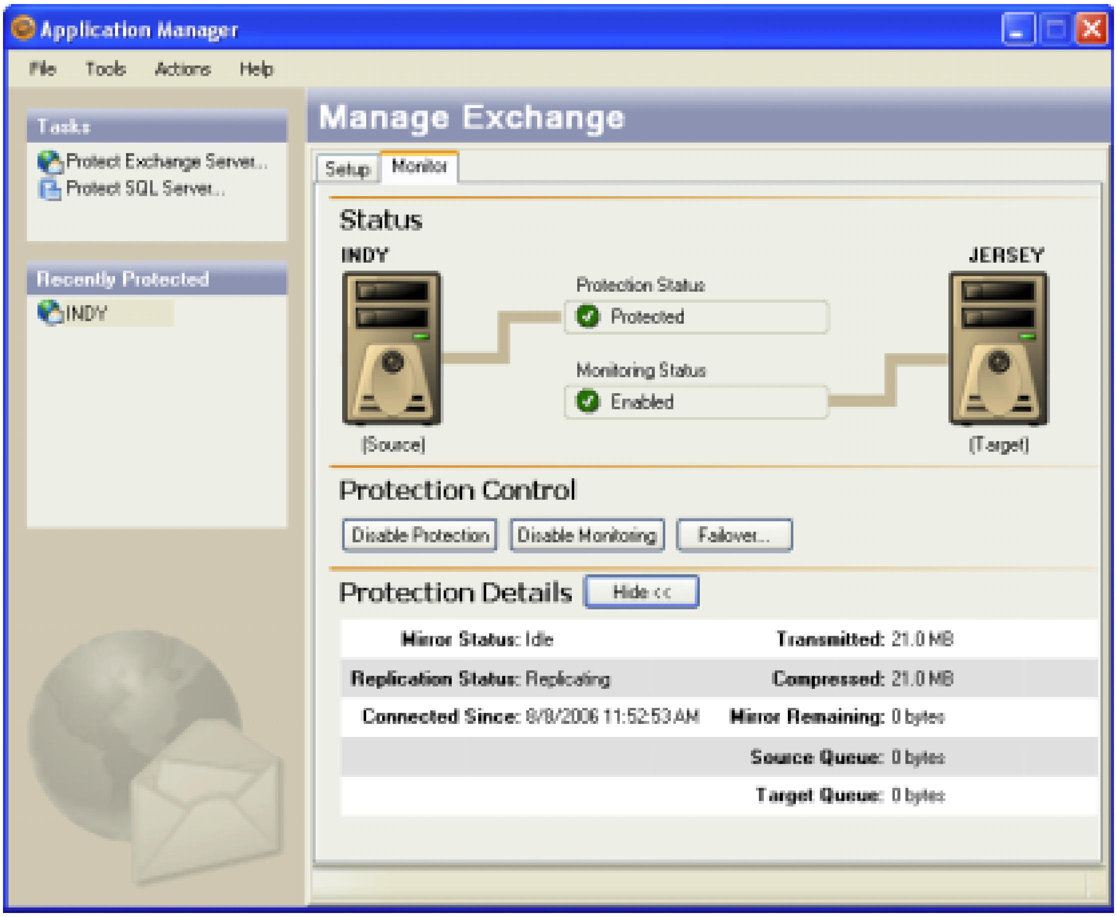
NOTE:

- If you run a validation against a source/target pair that is in a Protected state and the validation detects issues with the target (such as the target is missing or contains incorrect SQL data), the **Fix** or **Fix All** button will be disabled. You must disable protection for the source/target pair before you can fix the issue. Then, you can re-enable protection.
- If the IP address(es) for the source or target server have changed since you originally configured protection (for example, if you configure the source or target in a staging area and then send it to a production location), you must re-configure the protection settings. When you are prompted to re-use the previous protection configuration, click **No**, then click the **Configure Protection** button.

Enabling Protection for a Server

Based on the current protection status, the **Enable/Disable Protection** button (on both the **Setup** and **Monitor** tabs) and menu options will be updated to display the available actions. If the Application Manager is not in a state that will allow protection to be enabled, the Enable/Disable Protection button and menu option will be grayed out (disabled).

After monitoring has been enabled for a source/target pair, you can view the status of the monitored connection on the **Monitor** tab.



Protection Status: Protected

Monitoring Status: Enabled

Mirror Status: Idle	**Transmitted:** 21.0 MB
Replication Status: Replicating	**Compressed:** 21.0 MB
Connected Since: 8/8/2006 11:52:53 AM	**Mirror Remaining:** 0 bytes
	Source Queue: 0 bytes
	Target Queue: 0 bytes

You can click the **Show/Hide** button to display or hide details about the protected pair.

For details about changing the units used to display bytes remaining in the mirror and queues, see Changing Storage Mirroring Application Manager preferences, page 11.

Enable protection

Click **Enable Protection**, or select **Actions, Enable Protection**. If you have not already performed a validation check, if you have changed the domain, source, target, or configuration parameters, or if you have disabled the connection, you will be prompted to run a validation check at this time. The Protection Status field will display the current status of the connection. When the initial mirror has completed, the Protection Status will change to “Protected” and, if you have not manually un-selected “Failover Enabled”, the Monitoring Status will change to “Enabled”.

A source server can have a “Protected” status only if the source is currently connected to a target and an Application Manager-generated replication set exists (named `xdag01` for Exchange, or `sqldag01` for SQL). While there may be other Storage Mirroring connections between the selected source and target, Application Manager only recognizes connections that it has created.

Any connection that has been built by Application Manager will be recognized as a valid connection, regardless of the connection state.

Disable protection

You can disable an existing Application Manager-generated source/target connection monitor within the Application Manager.

You must disable protection before you can change any of the Application Manager configuration parameters.

1. If you select a source that is already protected in the **Source Server** field, the target server will be filled in automatically and the Protection Status should indicated "Protected".
2. Click **Disable Protection** at the bottom of the window, or select **Actions, Disable Protection**, to disable protection.

Monitor protection status

After the initial mirror, your source server is protected.

To change whether failover monitoring is enabled, click the **Enable/Disable Monitoring** button at the bottom of the window, or select either **Enable Monitoring** or **Disable Monitoring** from the **Actions** menu.

NOTE: You cannot use both the Failover Control Center and the Storage Mirroring Application Manager interfaces to monitor a source/target pair at the same time. Hewlett-Packard recommends that all monitoring occur from the Application Manager interface. If both interfaces are open and a failover condition occurs, failover will not be initiated until the failover prompt is cleared in both interfaces.

Verify target data viability (Exchange only)

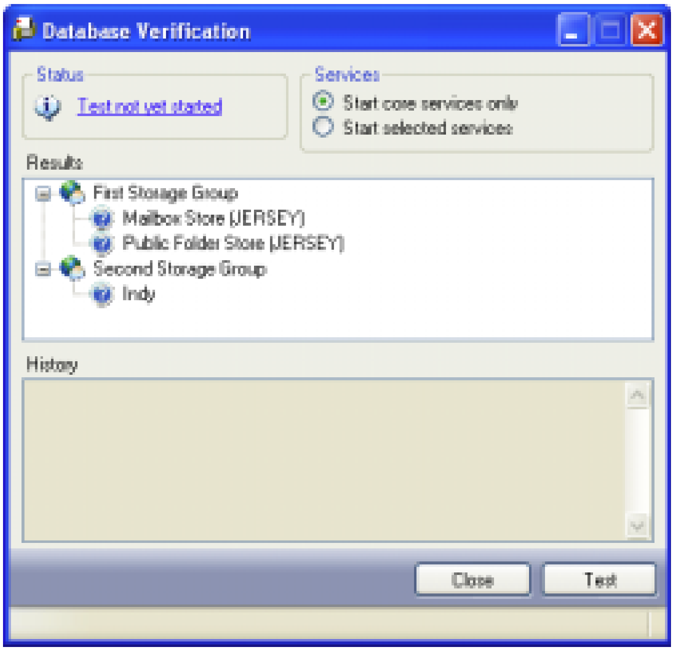
After you have configured your servers, you can use the Storage Mirroring Application Manager to run a test that verifies that the database on the target is viable for failover. One benefit of performing the verification test is that you do not have to perform an additional remirror or failover to verify target data viability.

In order to perform a database verification, the following prerequisites must be met:

- The target server must be running Windows 2003, Service Pack 1 or later.
- No Exchange data can reside on the system volume. (This is because the system volume cannot be reverted from a snapshot.) See Relocating the SMTP pickup path and queues, page 41.
- If you are running the Storage Mirroring Application Manager from any server other than the source or target, you must install the Exchange System Manager component on that server (due to a dependency on the `cdo.dll` file).
- If the current volumes do not have adequate space to contain the snapshots, modify the properties for the Shadow Copies settings on each volume to set the storage location of the snapshots where the Exchange data resides.

While in verification mode, Storage Mirroring will queue on the target in the directory you selected during Storage Mirroring configuration. You should be aware of your data change rate and make sure you have adequate capacity on the volumes configured for the Storage Mirroring target queues. For more information, see the Storage Mirroring *User's Guide*.

You can verify the target stores at any time following the successful completion of a mirror. When you select **Actions, Verify Target Data**, the following window will appear:



Database Verification

Status: Test not yet started

Services:
● Start core services only
○ Start selected services

Results:
- First Storage Group
  - Mailbox Store (JERSEY)
  - Public Folder Store (JERSEY)
- Second Storage Group
  - Indy

The Database Verification window includes the following controls and indicators:

- **Status**—The overall status of the database verification. Click on the status description for more information.
- **Services**—Select whether you want to start only the core application services, or all of the services you selected on the Failover tab when you configured protection. The **Start Selected Services** option would be used to include application add-ons such as Blackberry or Anti-Virus when configured with failover.
- **Results**—Displays the status of the target Exchange Stores and Storage Groups. Initially, the state of the Stores and Storage Groups is unknown (indicated by a question mark icon); it will change to green when the stores have successfully mounted.
- **History**—A log showing the sequence of events.
- **Current activity**—During the validation test and protection restoration, the status messages at the bottom of the screen describe the test progress.

To verify the target data, click the **Test** button. You will see the **History** window updated as the test proceeds. The **Status** field will display “Starting test” while preparing the target. When the stores finish mounting, the **Status** field changes to “Target online”. At this point, the verification is complete and the target application is ready for any other custom testing. You **must** click the **Continue** button to revert the target to the pre-test state and transition out of testing mode.

Relocating the SMTP pickup path and queues

Follow these steps to relocate the SMTP pickup path and queues on the source prior to enabling protection and propagating changes to the target using cloning.

1. Open `ADSIEdit.mmc` (available from the Windows Server Support Tools).
2. Right-click on **ADSI Edit** in the left pane and select **Connect to**.
3. In the **Select Well Known Naming Context**, choose **Configuration**.
4. For the MTA Path:
   a. Drill down by double-clicking at each level to the following path (substituting your environment configuration):

   ```
   CN=Microsoft MTA,CN=Source_Server,CN=Servers,CN=First Administrative
   Group,CN=Administrative Groups,CN=NewTestOrg,CN=Microsoft
   Exchange,CN=Services,CN=Configuration,DC=DTAMTest,DC=com
   ```
   b. Right-click the `MTA` object and select **Properties**.

   c. Scroll down to the `msExchMTADatabasePath` and double-click to edit. Set to a drive other than system.

5. For the SMTP Queues:
   a. Drill down by double-clicking at each level to the following path (substituting your environment configuration):

      ```
      CN=SMTP_Virtual_Server_Name,CN=SMTP,CN=Protocols,CN=Source_Server,CN=Servers,
      CN=First Administrative Group,CN=Administrative
      Groups,CN=NewTestOrg,CN=Microsoft
      Exchange,CN=Services,CN=Configuration,DC=DTAMTest,DC=com.
      ```

   b. Right-click the `SMTP_Virtual_Server_Name` object and select **Properties**.
   c. Scroll down to the `msExchSmtpQueueDirectory` and double-click to edit. Set to a drive other than system.
   d. Scroll down to the `msExchSmtpPickupDirectory` and double-click to edit. Set to a drive other than system.
   e. Repeat steps a-d for each SMTP Virtual server.
6. Repeat steps 4 and 5 for the target server, or select **Disable Protection**, run **Validation**, and choose to **Fix** the related issues found.

Failover, Failback, and Restoration

If you selected DNS failover, you can use the Application Manager to automate failover, failback, and restoration. If you selected Identity failover, you will need to use the manual processes described in Identity failover, failback, and restoration, page 45.

DNS failover, failback, and restoration

Based on the current protection status and/or failover state, the **Failover/Failback** button on the Monitor tab and menu options will be updated to display the available command. If the Application Manager is not in a state that will allow failover or failback to be executed, the **Failover/Failback** button and menu option will be grayed out (disabled).

In the Application Manager, there are two ways that failover can be initiated:

- Automatically, when a failover condition has been met (such as if the source has gone down)
- Manually (for instance, when you want to do maintenance or upgrades on the source server)

In order to initiate either an automatic or manual failover, the source and target servers must already be configured so that the Protection Status is “Protected” and Monitoring Status is “Enabled”.

During failover and failback, the status messages at the bottom of the screen describe the failover or failback progress.

NOTE:

- Protection Status and Monitoring Status on the main screen are not updated during failover and failback.
- The refresh update rate is not automatically updated during failover and failback.

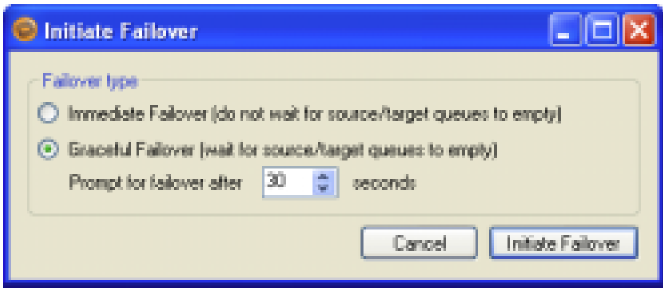
Initiating automatic failover

When the **Manual Intervention Required** option is selected on the Failover tab of the Configure Protection window, a prompt will occur when a failover condition is met. For more information about setting failover options, see Failover settings, page 16.

If you cleared the **Manual Intervention Required** option and have failover enabled for your server pair, failover will occur automatically when a failover condition is met.

Initiating manual failover

To initiate a manual failover, select **Actions, Failover**, or click the **Failover** button on the Monitoring tab. The Initiate Failover box will appear.



Initiate Failover

Failover type

○ Immediate Failover (do not wait for source/target queues to empty)

● Graceful Failover (wait for source/target queues to empty)

Prompt for failover after 30 seconds

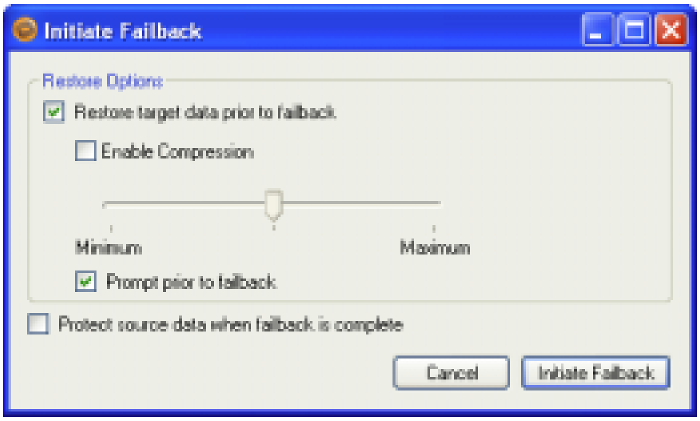
Select either **Immediate Failover** (to begin failover immediately and not wait for the queues to empty), or **Graceful failover** (to wait for the target queue to empty before failing over). The queues could contain any messages or data recently sent to the target from the source. If the queues aren’t empty when the prompt delay is reached, you will be asked whether you want to continue waiting, or to failover immediately.

Click **Initiate Failover** to begin failover process. After you select **Initiate Failover**, the failover process will begin. You cannot cancel or interrupt this process.

Failback and restoration

After issues on source server are resolved and it is connected and online, fail back to the source and restore any modified data. In order to initiate failback, both the Protection Status and Failover/Monitoring Status must be "Failed Over".

To initiate failback, click the **Failback** button, or select **Actions, Failback**. The Initiate Failback window will appear.



☑ Restore target data prior to failback

□ Enable Compression

☑ Prompt prior to failback

□ Protect source data when failback is complete

On the Initiate Failback window, select the following failback options:

- **Restore target data prior to failback**—Select this option if you want to restore any modified data from the target back to the source prior to beginning the failback.
- **Enable Compression**—Select this option to enable compression of data that is transmitted from the target to the source. Then, set the level from minimum to maximum compression. The default level is inherited from the source-to-target connection.
- **Prompt prior to failback**—Select this option if you want a prompt to appear before failing back.
- **Protect source data when failback is complete**—Select this option if you want to automatically re-enable protection for the source after the failback is complete. You will be prompted to verify that the source has been restored successfully before the protection of the source data is re-enabled.

Click **Initiate Failback** to begin the failback process. The restoration will begin, and the Protection Status will display the progress of the restoration. If you selected **Prompt prior to failback**, when the restoration is complete a prompt will appear asking if you want to failback. Click **Yes** to fail back to the source.

During restoration, the Application Manager will display the percent complete.

NOTE: This note applies to using the Storage Mirroring Application Manager with Exchange on Windows 2000 clusters.

If the owning node of the Exchange virtual server changes on the target cluster while the source is in a failed over state, the failed over state information will be lost. Consequently, the user will have to manually failback and restore their data. You will need to perform the following steps:

If the original owning node (the owning node at the time of failover) is still available:

1. Move the Exchange virtual server to that node.
2. Restart the Application Manager.
3. Select the source and target servers.
4. Failback.

If the original owning node is not available:

1. Disconnect the source-to-target server connection.
2. Create a connection in the Storage Mirroring Management Console from the target owning node to the source server owning node that includes the protected Exchange data.
3. After the mirror is complete, disconnect the connection.
4. Remove the Deny ACE entry for the cluster administrator from the source server's DNS object in Active Directory.
5. Run the pre_failback.bat script in the Storage Mirroring installation directory on the target owning node.
6. Run the post_restore.bat script in the Storage Mirroring installation directory on the source owning node.

Identity failover, failback, and restoration

The following sections describe the manual processes you can use to manage failover, failback, and restoration. These manual processes are required if you chose to perform Identity failover.

You will be using the Storage Mirroring Management Console, Failover Control Center, and/or Text Client to manage identity failover and failback. For more information about using Storage Mirroring, refer to the Storage Mirroring *User's Guide*.

Initiating a failover

If a failure occurs and the Failover Control Center Time to Fail counter reaches zero (0), a dialog box will appear in the Failover Control Center requiring user intervention to initiate failover. (If the Failover Control Center is not open when the failure occurs, the dialog box will appear the next time the Failover Control Center is opened and you are logged on to the target. See the Storage Mirroring *User's Guide* for information on monitoring a failure.) Acknowledge the manual intervention prompt to start failover.

The post-failover script created earlier will automatically run. During failover, Windows Event Viewer, the Storage Mirroring log, DFO log, and Storage Mirroring Application Manager logs (both log files are located in the same directory as the Storage Mirroring Application Manager) record the failover events. When failover is complete, the target will have the application services started, the databases mounted, and the users pointed to the target.

NOTE: If you are failing over Exchange, after the changes have propagated through your environment, clients can connect through Outlook® or Outlook Web Access to receive their e-mail. Users that had Outlook open during the failure will need to restart the Outlook client (excluding Outlook Web Access clients on a LAN).

If DNS failover was selected, the clients will have to wait for the IP cache to expire, or type in “`ipconfig /flushdns`” in a command window. This time can be adjusted by lowering the TTL (Time to Live) setting within your DNS server’s configuration. For more information, refer to your DNS server documentation.

Failback and restoration

If your source experiences a failure, such as a power, network, or disk failure, your target machine will stand in for the source while you resolve the source machine issues. During the source machine downtime, data is updated on the target machine. When your source machine is ready to come back online, the data is no longer current and must be updated with the new data on the target machine.

Before you begin to restore to the original source, resolve the issue(s) that caused the failure.

Recovering to the original source

1. After repairing/rebuilding the source server offline, bring the server up but leave the network connection disabled by unplugging the cable or disabling the network interface adapter.
2. Stop all of the services on the source so that you can overwrite the data with the newer data on the target. Because the source server cannot communicate with a domain controller because its network connection is still inactive, this will take longer than normal. The following table lists the services that must be stopped, in the order in which they must be stopped. Stop the services appropriate to your application.

Exchange	SQL
MSExchangeSA	MSSqlServer
MSExchangeMGMT	SQLServerAgent
POP3SVC	MSSearch (SQL 2000)/MSFteSQL (SQL 2005)
IMAP4SVC	MSSQLServerADHelper
ResVC	MSDTC
MSExchangeES	MSSQLServerDLAPService
W3SVC	MSDTSServer
SMTPSVC	SQLWriter

3. On the target, open the Failover Control Center (**Start**, **Programs**, **Storage Mirroring**, **Failover Control Center**).
4. Double-click the target machine that is currently standing in for the failed source to login.
5. Highlight the failed source and click **Failback**. The failback script created earlier will automatically run. During failback, Windows Event Viewer and the Storage Mirroring log record the failback events. When failback is complete, the services will be stopped on the target and the Failback Complete dialog box will appear.
6. **Do not** select **Continue** or **Stop** at this time. First, reconnect the source to the network.
7. After the source is available on the network, select **Continue** (to restart monitoring) or **Stop** to disable monitoring.
8. To begin the restoration process, open the Storage Mirroring Management Console on the target (**Start**, **Programs**, **Storage Mirroring**, **Management Console**).
9. Login to the source machine by double-clicking on it.
10. Right-click on the original connection (`xdag01` for Exchange, or `sqldag01` for SQL) and select **Disconnect**.
11. Select **Tools**, **Restoration Manager**.
12. Complete the appropriate fields on the Restoration Manager.
    - **Original Source**—The source where the data originally resided.
    - **Restore From**—The target that contains the replicated data that users have been updating.
    - **Replication Set**—The name of the replication set
    - **Restore To**—The source where the data will be restored to.
13. Disable **Only if backup copy is more recent**. This option must be disabled because if the services were stopped on the source after the time they were stopped on the target, the source files will have a more recent date and time and the target files will not be restored.

14. Identify the correct drive mappings for the data and any other restoration options necessary. For detailed information on the restoration options, see the Storage Mirroring *User's Guide*.
15. **On the Orphans tab, select to move or delete orphan files on the source.** Orphan files, such as out-dated transaction logs, may keep the database from starting on the source. For more information about orphan files, see the Storage Mirroring *User's Guide*.
16. Verify that the selections you have made are correct and click **Restore**. The restoration procedure time will vary depending on the amount of data that you have to restore.

    When the restoration process is complete, the restoration status information will no longer appear in the right pane.
17. If you are performing a failback for an Exchange server, continue to the next section, Rehoming the Exchange objects to the source, to complete the restoration process.

    If you are performing a failback for a SQL server, continue to Re-enabling protection, page 47 to complete the restoration process.

Rehoming the Exchange objects to the source

After the restoration is complete, you will need to run the Exchange Failover utility (`exchfailover.exe`) to rehome the informational store databases to the source. For more information about using the Exchange Failover utility, see Appendix F: Using the Exchange Failover (EFO) Utility, page 73.

1. From a command prompt on the source, run the `post_restore.bat` file that Application Manager automatically generated.
2. Restart any Outlook clients so that they can access the source.

To re-establish protection of the Exchange data on the source, create a replication set, re-establish the Storage Mirroring connection to the target, and begin failure monitoring as documented earlier in the procedure.

If DNS failover was selected, the clients will have to wait for the IP cache to expire, or type in “`ipconfig /flushdns`” in a command window. This time can be adjusted by lowering the TTL (Time to Live) setting within your DNS server’s configuration. For more information, refer to your DNS server documentation.

Re-enabling protection

To re-enable protection for your source, repeat the steps in Protecting an Exchange Server, page 13 or Protecting a SQL Server, page 25.

You can click the **Enable Protection** button to re-enable protection for the same source/target pair.

Appendix A: Recommended Credentials

Proper user credentials must be assigned in order for a configuration to be valid. If these credentials are not properly assigned, you will be prompted to enter alternate credentials before protection can be enabled.

1. The user must be a member of the “Power Users” group on the client machine.
2. The user must be a member of both servers’ local “Storage Mirroring Admin” group.
3. The user must be a member of the “Domain Admins” group for the domain in which the source’s DNS server resides.
4. The user must be a member of the local “Administrators” group on each Exchange or SQL server.
5. The user must have Full Control on the WMI DNS Namespace on the source's primary DNS server.
6. The user must be a member of the domain's “DnsAdmins” group where the source's primary DNS server is located.
7. **Exchange only:** The user must be an “Exchange Full Administrator”.
8. **SQL only:** The user must be assigned the “System Administrator” role on the SQL server.

For more information about how to assign each of these credentials, see the following sections.

Assigning the user to the Power Users group

1. Select **Start, Settings, Control Panel**. Double-click **Administrative Tools**, then double-click **Computer Management**.
2. In the left pane, select the **Groups** folder (located under **Computer Management\System Tools\Local Users and Groups**).
3. Right-click the **Power Users** group, then select **All Tasks, Add to Group**.
4. Click **Add**.
5. In **Location**, click the domain containing the users and computers you want to add, then click **OK**.
6. In **Name**, type the name of the user you want to add to the group. If you want to validate the user or group names that you are adding, click **Check Names**.
7. Click **OK** to close all open dialog boxes.

Assigning the user to the Storage Mirroring Admin group

Users that need administrator access to Storage Mirroring must be added to the Storage Mirroring Admin group.

1. Select **Start, Settings, Control Panel**. Double-click **Administrative Tools**, then double-click **Computer Management**.
2. In the left pane, select the **Groups** folder (located under **Computer Management\System Tools\Local Users and Groups**).
3. Double-click the **Storage Mirroring Admin** group.
4. To add a user to the group, click **Add**.
5. Select the user to be included in the Storage Mirroring Admin group.
6. Click **OK** to return to the Local Group Properties dialog box.
7. Click **OK** to return to the User Manager.
8. Exit the User Manager.

Assigning the user to the Domain Admins group

Follow these steps to add a user to the domain Domain Admins group for the source’s DNS server.

1. Select **Start, Programs, Administrative Tools**, **Active Directory Users and Computers**.
2. Right-click the **Domain Admins** group and select **Properties**.
3. Select the **Members** tab.
4. To add a user to the group, click **Add**.
5. In **Location**, click the domain containing the users you want to add, then click **OK**.
6. In **Name**, type the name of the user you want to add to the group. If you want to validate the user or group names that you are adding, click **Check Names**.

7. Click **OK** to close all open dialog boxes.

Assigning the user to the local servers' Administrators group

Follow these steps to add a user to the Administrators group on each server.

1. On the first server, select **Start, Settings, Control Panel**. Double-click **Administrative Tools**, then double-click **Computer Management**.
2. In the left pane, select the **Groups** folder (located under **Computer Management\System Tools\Local Users and Groups**).
3. Right-click the **Administrator** group and select **Properties**.
4. If the user is not already a member of the Administrators group, click **Add**.
5. In **Location**, click the domain containing the users you want to add, then click **OK**.
6. In **Name**, type **Administrator**.
7. Click **OK** to close all open dialog boxes.
8. Repeat for each additional server.

Assigning Full Control on the WMI DNS Namespace

Following validation, there will be a message stating the DNS WMI provider cannot be contacted. This is a false message because DNS Validation passed so it can be ignored. This message does not appear if the user is a member of the "Domain Admin" group for the domain where the DNS server resides.

1. Click **Start, Run**, and type `MMC`. Click **OK**.
2. Select **File, Add/Remove Snap-in**.
3. Click **Add** and select **WMI Control**.
4. Click **Add**, then click **Finish**.
5. Click **Close**, then click **OK**.
6. Right-click **WMI Control** and select **Properties**.
7. Select the **Security** tab.
8. Double-click on **Root** to expand the tree.
9. Select **MicrosoftDNS**, then click the **Security** button.
10. Verify that the user is in the ACL list with the following permissions. If the permissions are not assigned, proceed to the next step.
    - Execute Methods
    - Full Write
    - Partial Write
    - Provider Write
    - Enable Account
    - Remote Enable
    - Read Security
11. Click **Add,** then enter the login name for the user account that will be opening Storage Mirroring Application Manager.
12. Click **OK** to close all open dialog boxes.
13. Restart the **Windows Management Instrumentation** service.

Assigning the user to the DnsAdmins group

Follow these steps to add a user to the domain DnsAdmins group.

1. Select **Start, Programs, Administrative Tools (Common), Active Directory Users and Computers**.
2. Right-click the **DnsAdmins** group and select **Properties**.
3. Select the **Members** tab.
4. To add a user to the group, click **Add**.
5. In **Location**, click the domain containing the users you want to add, then click **OK**.

6. In **Name**, type the name of the user you want to add to the group. If you want to validate the user or group names that you are adding, click **Check Names**.
7. Click **OK** to close all open dialog boxes.

Assigning Exchange Full Administrator permission

1. Select **Start, Programs, Microsoft Exchange, System Manager**.
2. Right-click on the organization name (at the top of the tree) and select **Delegate Control**.
3. The Exchange Delegation Tool will open. Click **Next**.
4. If the user is not listed as Exchange Full Administrator, click **Add**.
5. Click **Browse**.
6. Type in the domain user's login name, then click **OK**.
7. Change the role to **Exchange Full Administrator**, then click **OK**.

Assigning SQL Server System Administrators permission

1. Start SQL Server Enterprise Manager (SQL Server 2000) or SQL Server Management Studio (SQL 2005).
2. Expand the **Security** folder under the server.
3. Select **Logins**.
4. Create a login for the user, if one does not already exist.
5. Select **Server Roles**.
6. Double-click the **System Administrators** (SQL Server 2000) or **sysadmin** (SQL Server 2005) role.
7. Click **Add**, select the user, and click **OK**.
8. Click **OK** on the Server Role Properties dialog box to save the change.

Appendix B: Exchange Failover with Blackberry

If you are using a standalone Blackberry server with Exchange, complete the following steps so that the Blackberry server will recognize when the Exchange server that has the BESAdmin account has been failed over.

1. Prior to failing over, shut down the Blackberry server.
2. After failover, bring the Blackberry server back up.
3. Open a command prompt on the Blackberry server and cd to `C:\Program Files\Research In Motion\BlackBerry Enterprise Server\Utility`.
4. Run the command `handheldcleanup –m`
5. Run the command `handheldcleanup –u`

   This command will prompt you for the name of the Blackberry server.

The same process should be followed when failing back.

Configuring Blackberry services for failover

To configure your Blackberry services to fail over with Exchange, the following Blackberry services should be added to the list of services to start/stop from the Failover tab when you configure protection.

- Blackberry Alert
- Blackberry Attachment Service
- Blackberry Controller
- Blackberry Dispatcher
- Blackberry Mobile Data Service
- Blackberry Policy Service
- Blackberry Router
- Blackberry Synchronization Service

NOTE: The services you need to add may vary based on your environment.

Appendix C: Exchange Validation Messages

The following table describes the validation checks that are performed to verify the connection.

Validation Message	Error/ Warning	Auto-Fix Available?
Storage Mirroring version		
"The Storage Mirroring version on the server <Server Name> cannot be used with the Storage Mirroring Application Manager" The version of Storage Mirroring on the designated server cannot be used with the Application Manager. The Application Manager requires at least Storage Mirroring version 4.4.0.	Error	No
"The Storage Mirroring versions on the source and target servers are not compatible" The version of Storage Mirroring on the source and target do not match and are not compatible.	Error	No
"The Storage Mirroring version on the server <Server Name> could not be determined" The version of Storage Mirroring on the designated server could not be determined. Verify that its version is at least 4.4.	Error	No
Operating system version		
"The OS version on the server <Server Name> is not valid" The operating system version on the designated server is not compatible with the Storage Mirroring Application Manager. Windows 2000 or later is required on each server.	Error	No
"The OS version on the source server <Server Name> and target server are not compatible for failover" The operating system versions on the source and target servers do not match and are not compatible for failover.	Error	No
Exchange version		
"The version of Exchange on the source and target do not match" The version of Exchange on the source and target do not match and are not compatible.	Error	Yes
Exchange Failover utility (EFO)		
"The Exchange Failover Utility is not available on the server <Server Name>" The Exchange Failover Utility file (exchfailover.exe) is not available on the designated server. This utility is needed to move users between the target and source during restore. This utility is provided with the Storage Mirroring Application Manager installation and should be copied to the server before continuing.	Error	Yes
"A later version of the Exchange Failover Utility is available for the server <Server Name>" The Exchange Failover Utility file is not the latest version. The latest version is provided with the Storage Mirroring Application Manager installation and should be copied to the server before continuing.	Error	Yes
DNS Failover utility (DFO)		
"The DNS Failover Utility is not available on the server <Server Name>" The DNS Failover Utility is not available on the designated server. This utility is needed to move DNS entries between the source and target on failover/failback. This utility is provided with the Storage Mirroring Application Manager installation and should be copied to the server before continuing.	Error	Yes
"A later version of the DNS Failover Utility is available for the server <Server Name>" The DNS Failover Utility is not the latest version. The latest version is provided with the Storage Mirroring Application Manager installation and should be copied to the server before continuing.	Error	Yes

Validation Message	Error/ Warning	Auto-Fix Available?
Account credential		
“Storage Mirroring is configured to run under a user account on the source server `<Server Name>`” Storage Mirroring is configured to run under a user account on the source server. It is recommended that Storage Mirroring be run under the **LocalSystem** account.	Warning	No
“Storage Mirroring is configured to run under a user account on the target server `<Server Name>`” Storage Mirroring is configured to run under a user account on the target server. It is recommended that Storage Mirroring be run under the **LocalSystem** account.	Warning	No
Login access		
“Unable to get login information for the Storage Mirroring service on source server `<Source Server Name>`” Unable to get login information for the Storage Mirroring service on the source server. Verify that the server is up, Storage Mirroring is running, and IP connectivity.	Error	No
“Unable to get login information for the Storage Mirroring service on target server `<Target Server Name>`” Unable to get login information for the Storage Mirroring service on the target server. Verify that the server is up, Storage Mirroring is running, and IP connectivity.	Error	No
Server access/permission		
“Cannot access directories on server `<Server Name>` via standard administrative shares” The designated server cannot be accessed via standard administrative shares (C$, D$, etc.). This is needed in order to write failover/failback scripts to the server. Make sure an administrative share (for example, 'C$') exists on the volume in which post-restore scripts will be stored.	Error	No
“Source server `<Source Server Name>` does not have permissions to update the Offline Address Book(s) on failover” The source server does not have sufficient privilege within the domain to update the Offline Address Book(s) location during failover and failback. This will prevent failover from functioning properly. You must update the appropriate permissions in Active Directory before proceeding.	Error	Yes
“Target server `<Target Server Name>` does not have permissions to update the Offline Address Book(s) on failover” The target server does not have sufficient privilege within the domain to update the Offline Address Book(s) location during failover and failback. This will prevent failover from functioning properly. You must update the appropriate permissions in Active Directory before proceeding.	Error	Yes
“Target server `<Target Server Name>` does not have permissions to update SPNs on failover” The target server does not have sufficient privilege within the domain to update Service Principal Names (SPNs) for the source on failover. This will prevent failover from functioning properly. You must update the appropriate permissions (ValidateWritesToSPN, ReadSPN, and WriteSPN) in Active Directory before proceeding.	Error	Yes

Validation Message	Error/ Warning	Auto-Fix Available?
“Target server <Target Server Name> does not have permissions to update the Exchange Routing Master on failover” The target server does not have sufficient privilege within the domain to update the Routing Master for the source on failover. This will prevent failover from functioning properly. You must update the appropriate permissions in Active Directory before proceeding. These rights include CreatemsExchRoutingGroupContainer, DeletemsExchRoutingGroupContainer, ReadmsExchRoutingGroupMembersDN, and WritemsExchRoutingGroupMembersDN.	Error	Yes
“Target server <Target Server Name> does not have permissions to update the Recipient Update Service on failover” The target server does not have sufficient privilege within the domain to update the Recipient Update Service for the source on failover. This will prevent failover from functioning properly. You must update the appropriate permissions in Active Directory before proceeding.	Error	No
Storage Mirroring connection		
“A connection already exists from the target to the source” Replication is already configured from the target to the source. This configuration will cause circular replication and is not permitted. Disable the connection between the target and source before proceeding.	Error	Yes
“A failover monitor already exists for this source/target pair” A failover monitor already exists for this source/target pair. Another monitor cannot be created for the same source/target pair, so Exchange-specific failover actions cannot be enabled. Disable the other monitor before proceeding.	Error	Yes
“A failover monitor does not exist for this connection” A failover monitor does not exist for this source/target pair, even though there is a connection between the servers to protect Exchange. This may be because the failover option was not selected when creating this connection. If you want to enable failover for this source/target pair, disable then re-enable the connection with the failover option selected.	Warning	No
“The target is in a 'Restore Required' state” A failover has previously occurred between the source and target, and data may need to be restored from the target. If you enable protection, the target data will be overwritten by the data from the source.	Warning	No
DNS WMI		
“The DNS WMI Provider is not available on server <Source DNS Server Name>” The DNS WMI Provider is not available on the source DNS server. This provider is required to move DNS entries during failover. The DNS WMI Provider is installed by default on Windows 2003 servers and may be downloaded from Microsoft for Windows 2000 servers.	Error	No
DNS failover		
“Reverse lookup is not enabled” A reverse lookup zone has not been created for this subnet within the DNS server. Microsoft recommends reverse lookup zones for proper Exchange operation.	Warning	No
“DNS Failover: Configuration Validation Failed” The DNS Failover utility was unable to access a DNS server containing source-related DNS resource records. This issue can be caused by incorrect configuration settings, including use of relative DNS server name in failover/failback scripts, incorrect DNS server FQDN in failover/failback scripts (for example, use of secondary instead of primary DNS server FQDN), incorrect access credentials, and so on.	Warning	No

Validation Message	Error/ Warning	Auto-Fix Available?
"DNS Failover: DNS validation timeout" The DNS validation test was not completed within the allotted time (30 seconds). This generally indicates that specified DNS server is not accessible, though it could also be caused by network performance issues. Verify that the DNS WMI provider is installed and that the server is available before re-testing.	Warning	No
"DNS Failover: Invalid IP address (`xx.xxx.x.xx`) specified for failover" The IP address specified for DNS failover (xx.xxx.x.xx) does not match an IP address that DNS has for the source server. Select **None** for these source IP(s) or ensure the IP(s) are associated with the source server in DNS and retry the test.	Warning	No
"DNS Failover: Invalid DNS credentials" The username or password specified for DNS access are either invalid, or the user does not have sufficient privileges to modify DNS records. Make sure that the specified credentials are correct and that the specified user is a member of the DNS Admin group.	Warning	No
"DNS Failover: Cannot contact specified DNS server" The DNS server cannot be contacted. Make sure that the server name is correct and the server is available.	Warning	No
"DNS Failover: Cannot find source record in DNS" Cannot find a record in DNS server for the source server.	Error	No
"DNS Failover: Source IP address (xx.xxx.x.xx) specified for failover does not match the target virtual SMTP server IP" The source IP address specified for DNS failover has a corresponding target IP address that does not match the virtual SMTP server IP of the target server. The SMTP service may be unavailable after failover.	Warning	No
"Primary DNS server is unavailable" The primary DNS server is unavailable. The secondary DNS server will be used instead.	Warning	No
"DNS Failover: The source server's SMTP virtual server IP address `<IP Address>` will not be failed over." The source IP address is the virtual SMTP server IP address for the source server but is not selected to be updated in DNS upon failover. As a result, SMTP service may be unavailable after failover. The IP address should have a target IP address associated with it on the Configure DNS failover dialog.	Warning	No
"DNS Failover: IP failover setup is incomplete" At least one source IP address should be monitored and updated. From the main Application Manager window, click **Configure**, then click **Configure** for DNS failover. Ensure that at least one source IP address is checked and at least one target IP address is selected.	Error	No
"This machine may not be set up to use the correct DNS server." This machine is set up to use a DNS server (xx.xxx.x.xx) that differs from the DNS server (xx.xxx.x.xx) where updates will be made. This can cause serious connectivity issues during and after failover and failback. Verify the client machine's configuration, or modify the DNS server where updates will be made.	Warning	No
Identity failover		
"Identity failover is not recommended" The Identity failover method cannot be used with integrated failover and failback. DNS failover can be used with integrated failover and failback, reduces downtime, and provides other benefits. It is recommended for most environments.	Warning	No

Validation Message	Error/ Warning	Auto-Fix Available?
"Identity failover cannot be enabled unless at least one IP address is selected to be monitored" You have selected Identity failover, but no IP addresses are selected to be monitored. From the main Application Manager window, click **Configure**, then click **Configure** for Identity failover.	Error	No
"Identity failover is not recommended across different subnets" You have selected Identity failover. However, since the source and target are on different subnets, the source IP address will not be accessible after failover occurs. DNS failover is recommended for this configuration.	Warning	No
Advanced options		
"The Create Failover Monitor option has been disabled" The Create Failover Monitor option has been disabled for this connection while failover is enabled. This option should only be disabled for debugging purposes, and disabling it will prevent the proper setup of failover monitoring. To enable the Create Failover Monitor option, select the **Fix** button.	Warning	Yes
"The Create Failover Scripts option has been disabled" The Create Failover Scripts option has been disabled for this connection while failover is enabled. This option should only be disabled for debugging purposes, and disabling it will prevent the proper setup of failover monitoring. To enable the Create Failover Scripts option, select the **Fix** button.	Warning	Yes
"The Create Repset option has been disabled" The Create Repset option has been disabled for this connection. This option should only be disabled for debugging purposes, and disabling it will prevent the proper setup of Exchange protection. To enable the Create Repset option, select the **Fix** button.	Warning	Yes
"The Create Connection option has been disabled" The Create Connection option has been disabled for this connection. This option should only be disabled for debugging purposes, and disabling it will prevent the proper setup of Exchange protection. To enable the Create Connection option, select the **Fix** button.	Warning	Yes
Services		
"Service `<Service Name>` could not be found on the target" The designated service is missing from the target server. If this service is not available at failover time, Exchange or other applications may not start properly.	Error	No
"Unable to connect to target server `<Target Server Name>` to get service information" The designated target server could not be contacted in order to get service information. This information is needed to determine whether Exchange services are running on the target, which could cause problems with protection. Make sure you have sufficient rights to access the server. This message is displayed only once— not for each service.	Error	No
"Service `<Service Name>` is currently running on the target" The designated service is running on the target. This may prevent data from being written to the target, as the service may lock certain files. The service should be stopped on the target before enabling protection.	Error	Yes
"Service `<Service Name>` is currently set to start automatically on the target" The designated service is set to start automatically on the target server. If the target server is restarted, the service will be started which may prevent data from being properly protected as the service may lock certain files. The service should be set to start manually before enabling protection.	Warning	Yes

Validation Message	Error/ Warning	Auto-Fix Available?
Replication set		
“The current replication set is not complete” The current replication set is not complete. It does not include all directories required to protect Exchange. This error may be the result of the Exchange configuration being changed since the replication set was created. To update the replication set, disable then re-enable the connection.	Error	No
“A non-Exchange connection for the replication set exists” A non-Exchange connection for the replication set to the target server exists. After a failover and failback, data in this replication set that has been modified on the target may be overwritten. It is recommended that you make this data part of the Exchange replication set in the Configure Protection window, and disconnect this connection.	Warning	No
“The Checksum All option is not enabled on the server `<Server Name>`” The Checksum All option is not enabled on the designated server. For transactional databases such as Exchange, this option is required to ensure data integrity on failover. To enable checksum all, from the Storage Mirroring Management Console, right-click on the server and select **Properties**. On the Source tab, enable **Block Checksum All Files on a Difference Mirror** and click **OK**.	Warning	Yes
DT COM		
“The file `DTCOM.dll` is not available on the server `<Server Name>`.” The file `DTCOM.dll` is not available on the designated server. This DLL is required by the Application Manager. This DLL is provided with the Application Manager installation and should be copied to the server before continuing.	Error	Yes
“The file `DTCOM.dll` is not registered on the server `<Server Name>`.” The file `DTCOM.dll` is not registered on the designated server. This DLL is required by the Application Manager. This DLL is provided with the Application Manager installation and should be registered on the server before continuing.	Error	Yes
“A later version of the file `DTCOM.dll` is available for the server `<Server Name>`.” The file `DTCOM.dll` is not the latest version. The latest version is provided with the Application Manager installation and should be copied to the server before continuing.	Error	Yes
Capicom		
“The file `CAPICOM.DLL` is not available on the server `<Server Name>`” The `capicom.dll` file is not available on the designated server. This utility is needed to encrypt credentials necessary to run the DNS Failover Utility. This .dll is provided with the Storage Mirroring Application Manager installation and should be copied to the server before continuing.	Error	Yes
“The `CAPICOM.DLL` is not registered on the server `<Server Name>`” The `CAPICOM.DLL` file is not registered on the designated server. This DLL must be registered to encrypt credentials necessary to run the DNS Failover utility. This DLL is provided with the Storage Mirroring Application Manager installation and should be registered on the server before continuing.	Error	No
“A later version of the `CAPICOM.DLL` is available for the server `<Server Name>`” The `CAPICOM.DLL` file is not the latest version. The latest version is provided with the Storage Mirroring Application Manager installation and should be copied to the server before continuing.	Error	Yes
Exchange configuration		
“No storage groups have been selected” No storage groups have been selected to protect on the Connection tab of the Configure Protection window. Only general Exchange data will be protected.	Error	No

Validation Message	Error/ Warning	Auto-Fix Available?
"The storage group `<Storage Group Name>` is not present on the target server" The designated storage group is not present on the target server. The Application Manager can fix this issue by copying the source Exchange server configuration to the target server. Be aware that this will overwrite your target Exchange configuration, including any storage groups or information stores you may have created. For more information, refer to your Exchange documentation.	Error	Yes
"The mailbox store `<Storage Group Name>\<Database Name>` does not exist on the target" The designated mailbox store does not exist on the target server. The Application Manager can fix this issue by copying the source Exchange server configuration to the target server. Be aware that this will overwrite your target Exchange configuration, including any storage groups or information stores you may have created. For more information, refer to your Exchange documentation.	Error	Yes
"The public folder store `<Storage Group Name>\<Database Name>` does not exist on the target" The designated public folder store does not exist on the target server. The Application Manager can fix this issue by copying the source Exchange server configuration to the target server. Be aware that this will overwrite your target Exchange configuration, including any storage groups or information stores you may have created. For more information, refer to your Exchange documentation.	Error	Yes
"Circular logging is enabled on the source server for storage group `<Storage Group Name>`" Circular logging is enabled on the source server for the designated storage group. For information about fixing circular logging, refer to your Exchange documentation.	Error	No
"The Exchange MTA Path on the source and target does not match" The Exchange MTA Path on the source and target does not match. For information about changing the MTA Path, refer to your Exchange documentation.	Error	Yes
"The Exchange Pickup Path on the source and target does not match" The Exchange Pickup Path on the source and target does not match. For information about changing the Pickup Path, refer to your Exchange documentation.	Error	Yes
"The Exchange Queue Path on the source and target does not match" The Exchange Queue Path on the source and target does not match. For information about changing the Queue Path, refer to your Exchange documentation.	Error	Yes
"The system path for storage group `<Storage Group Name>` does not match on the source and target servers" The system path for the designated storage group does not match on the source and target servers. For information about changing the system path for the storage group, refer to your Exchange documentation.	Error	Yes
"The logfile path for storage group `<Storage Group Name>` does not match on the source and target servers" The logfile path for the designated storage group does not match on the source and target servers. For information about changing the logfile path for the storage group, refer to your Exchange documentation.	Error	Yes
"The logfile prefix for storage group `<Storage Group Name>` does not match on the source and target servers" The logfile prefix for the designated storage group does not match on the source and target servers. For information about changing the logfile prefix for the storage group, refer to your Exchange documentation.	Error	Yes

Validation Message	Error/ Warning	Auto-Fix Available?
“The Exchange database (EDB) path for the mailbox store ‘StorageGroupName’\‘DatabaseName’ does not match on the source and target servers” The Exchange database (EDB) path for the mailbox store in the designated storage group does not match on the source and target servers. For more information, refer to your Exchange documentation.	Error	Yes
“The Exchange streaming database (SLV) path for the mailbox store <Storage Group Name>\<Database Name> does not match on the source and target servers” The Exchange streaming database (SLV) path for the mailbox store in the designate storage group does not match on the source and target servers. For more information, refer to your Exchange documentation.	Error	Yes
“The Exchange database (EDB) path for the public folder store <Storage Group Name>\<Database Name> does not match on the source and target servers” The Exchange database (EDB) path for the public folder store in the designated storage group does not match on the source and target servers. For more information, refer to your Exchange documentation.	Error	Yes
“The Exchange streaming database (SLV) path for the public folder store <Storage Group Name>\<Database Name> does not match on the source and target servers” The Exchange streaming database (SLV) path for the public folder store in the designate storage group does not match on the source and target servers. For more information, refer to your Exchange documentation.	Error	Yes
“'Zero Data Pages During Backup' is enabled on the source server for the storage group ‘StorageGroupName’” 'Zero Data Pages During Backup' is enabled on the source server for the designated storage group. This Exchange option may result in large amounts of data being replicated between the source and target, which could impact overall system performance. It is recommended that this option be disabled.	Warning	No
Exchange clusters		
“Source account is not a member of the Storage Mirroring Admin group on the node <node name>. The account running the source cluster service (<account name>) is not a member of the Storage Mirroring Admin group on the target node <node name>. The connection will fail to be created when this node is the owning node of the Exchange virtual server.	Error	No
“The Storage Mirroring install path on the server <Server Name> does not match the install path of the owning node” The Storage Mirroring install path on the designated server does not match the install path of the owning node. All nodes on a cluster must have Storage Mirroring installed to the same location.	Error	No
“The OS version on the server <Server Name> is not valid” The OS version on the source node is not compatible with the Application Manager. Windows 2000 or later is required on each server.	Error	No
“Cannot access source node directories via standard administrative shares” The designated server cannot be accessed via standard administrative shares <Share Path>. This is needed in order to write post-restore scripts to the source server. Make sure an administrative share (e.g. 'C$') exists on the source on the volume in which post-restore scripts will be stored.	Error	No
“Resource <Resource Name> does not exist on the target” In order for protection to be successful, the selected resources must exist on the target server. The designated resource could not be found on the target cluster.	Error	No

Validation Message	Error/ Warning	Auto-Fix Available?
"Resource `<Resource Name>` is currently online on the target" The designated resource is online on the target. This may prevent data from being written to the target, as the resource and underlying service may lock certain files. The resource should be taken offline on the target cluster before enabling protection.	Error	Yes
"Resource `<Resource Name>` is currently set to be brought online automatically on the target" The designated resource is set to be brought online automatically on the target server. If the target server is restarted, the resource will be brought online which may prevent data from being properly protected as the resource may lock certain files. The resource should be set to be brought online manually before enabling protection.	Warning	Yes
"Exchange Network Name resource will be brought online if DNS registration fails." The Exchange Network Name resource `<Resource Name>` is currently configured to be brought online even if DNS registration fails. Application Manager will be unable to disable this resource. The ability to disable this resource ensures data integrity.	Warning	Yes
"The source server is an Enterprise Exchange server and the target is not." The source server is running an Enterprise version of Exchange and the target server is running a Standard version of Exchange. This can cause issues during failover if the source server has: • More than 1 mailbox store in a storage group. • More than 1 public folder store in a storage group. • The size of a single database exceeds 16 GB. Verify that none of these conditions apply before enabling protection.	Warning	No
"Source/target server `<server name>` does not have permission to update administrative group properties." The source/target server `<server name>` does not have permission to update certain AD properties (including administrative group properties) during failover and failback. The lack of this permission will also affect the ability to change the location of any offline address books hosted by the source server. This issue will prevent failover and failback from functioning properly.	Error	Yes

Appendix D: SQL Validation Messages

The following table describes the validation checks that are performed to verify the connection.

Validation Message	Error/ Warning	Auto-Fix Available?
Storage Mirroring version		
"The Storage Mirroring version on the server `<Server Name>` could not be determined" The version of Storage Mirroring on the designated server could not be determined. Verify that its version is at least 4.4.	Error	No
"The Storage Mirroring version on the server `<Server Name>` cannot be used with the Application Manager." The version of Storage Mirroring on the designated server cannot be used with the Application Manager. Storage Mirroring Application Manager requires at least version 4.4.0.	Error	No
"The Storage Mirroring versions on the source server `<Source Server Name>` and the target server `<Target Server Name>` are not compatible." The Storage Mirroring versions on the source and target servers do not match and are not compatible.	Error	No
Operating system version		
"The OS versions on the source server `<Source Server Name>` and target server `<Target Server Name>` are not compatible for failover." The operating system versions on the source and target servers do not match and are not compatible for failover.	Error	No
"The OS version on the server `<server name>` is not valid" The operating system version on the designated server is not compatible with the Storage Mirroring Application Manager. Windows 2000 or later is required on each server.	Error	No
SQL version		
"Source and target SQL Server versions don't match" The Protection Mode you have selected requires that the Source and target SQL Server versions (major, minor, and service pack levels) match. The source SQL version is: `<Version Number>`. The target SQL version is: `<Version Number>`	Error	No
DNS Failover utility (DFO)		
"The DNS Failover Utility is not available on the server `<Server Name>`" The DNS Failover Utility is not available on the designated server. This utility is needed to move DNS entries between the source and target on failover/failback. This utility is provided with the Storage Mirroring Application Manager installation and should be copied to the server before continuing.	Error	Yes
"A later version of the DNS Failover Utility is available for the server `<Server Name>`" The DNS Failover Utility is not the latest version. The latest version is provided with the Storage Mirroring Application Manager installation and should be copied to the server before continuing.	Error	Yes
Account access/login		
"Unable to get login information for the Storage Mirroring service on source server `<Source Server Name>`" Unable to get login information for the Storage Mirroring service on the source server. Verify that the server is up, Storage Mirroring is running, and IP connectivity.	Error	No
"Unable to get login information for the Storage Mirroring service on target server `<Target Server Name>`" Unable to get login information for the Storage Mirroring service on the target server. Verify that the server is up, Storage Mirroring is running, and IP connectivity	Error	No

Validation Message	Error/ Warning	Auto-Fix Available?
"Storage Mirroring is configured to run under a user account on the source server `<Source Server Name>`" Storage Mirroring is configured to run under a user account on the source server. It is recommended that Storage Mirroring be run under the **LocalSystem** account.	Warning	No
"Storage Mirroring is configured to run under a user account on the target server `<Target Server Name>`" Storage Mirroring is configured to run under a user account on the target server. It is recommended that Storage Mirroring be run under the **LocalSystem** account.	Warning	No
"The SQL Server service account on the source server `<Source Server Name>` is local" The SQL Server service account on the source server is a local user account. Only domain user and **LocalSystem** accounts can be used to start SQL Server when protecting the source server with the Application Manager. The source SQL Server service account must be changed.	Error	No
"The SQL Server service account on the target server `<Target Server Name>` is local" The SQL Server service account on the target server is a local user account. Only domain user and **LocalSystem** accounts can be used to start SQL Server when protecting the source server with the Application Manager. The target SQL Server service account must be changed.	Error	No
"The Storage Mirroring service account on the target server `<Target Server Name>` is local" The Storage Mirroring service account on the target server is a local user account. Only domain user and **LocalSystem** accounts can be used to start Storage Mirroring when protecting the source server with the Application Manager. The target Storage Mirroring service account must be changed.	Error	No
"The target server `<Target Server Name>` does not have permissions to update SPNs on failover" The designated target server does not have sufficient privilege within the domain to update Service Principal Names (SPNs) for the source on failover. This will prevent failover from functioning properly. You must update the appropriate permissions in Active Directory before proceeding.	Error	Yes
Server access		
"Cannot access source server directories via standard administrative shares" The designated server cannot be accessed via standard administrative shares `<Share Path>`. This is needed in order to write post-restore scripts to the source server. Make sure an administrative share (e.g. 'C$') exists on the source on the volume in which post-restore scripts will be stored.	Error	No
Storage Mirroring connection		
"A failover monitor already exists for this source/target pair" A failover monitor already exists for this source/target pair. Another monitor cannot be created for the same source/target pair, so SQL-specific failover actions cannot be enabled. Disable the other monitor before proceeding.	Error	Yes
"A failover monitor does not exist for this connection" A failover monitor does not exist for this source/target pair, even though there is a connection between the servers to protect SQL. This may be because the failover option was not selected when creating this connection. If you want to enable failover for this source/target pair, disable then re-enable the connection with the failover option selected.	Warning	No
"A connection already exists from the target to the source" Replication is already configured from the target to the source. This configuration will cause circular replication and is not permitted. Disable the connection between the target and source before proceeding.	Error	Yes

Validation Message	Error/ Warning	Auto-Fix Available?
“The target is in a 'Restore Required' state” A failover has previously occurred between the source and target, and data may need to be restored from the target. If you enable protection, the target data will be overwritten by the data from the source.	Warning	No
DNS WMI		
“The DNS WMI Provider is not available on server `<Source DNS Server Name>`” The DNS WMI Provider is not available on the source DNS server. This provider is required to move DNS entries during failover. The DNS WMI Provider is installed by default on Windows 2003 servers and may be downloaded from Microsoft for Windows 2000 servers.	Error	No
DNS failover		
“Reverse lookup is not enabled” A reverse lookup zone has not been created for this subnet within the DNS server. A reverse lookup zone is recommended.	Warning	No
“Primary DNS server is unavailable” The primary DNS server is unavailable. The secondary DNS server will be used instead.	Warning	No
“DNS Failover: DNS validation timeout” The DNS validation test was not completed within the allotted time (30 seconds). This generally indicates that specified DNS server is not accessible, though it could also be caused by network performance issues. Verify that the DNS server is available before re-validating.	Warning	No
“DNS Failover: Invalid IP address (`xx.xxx.x.xx`) specified for failover” The IP address specified for DNS failover (xx.xxx.x.xx) does not match an IP address that DNS has for the source server. Select **None** for these source IP(s) or ensure the IP(s) are associated with the source server in DNS and retry the test.	Warning	No
“DNS Failover: Invalid DNS credentials” The username or password specified for DNS access are either invalid, or the user does not have sufficient privileges to modify DNS records. Make sure that the specified credentials are correct and that the specified user is a member of the DNS Admin group.	Warning	No
“DNS Failover: Cannot contact specified DNS server” The DNS server `<Server Name>` cannot be contacted. Make sure that the server name is correct and the server is available.	Warning	No
“DNS Failover: Cannot find source record in DNS” Cannot find a record in DNS server `<Server Name>` for the source server.	Error	No
“DNS Failover: IP failover setup is incomplete” At least one source IP address should be monitored and updated. From the main Application Manager window, click **Configure**, then click **Configure** for DNS failover. Ensure that at least one source IP address is checked and at least one target IP address is selected.	Error	No
“DNS Failover: Configuration Validation Failed” The DNS Failover utility was unable to access a DNS server containing source-related DNS resource records. This issue can be caused by incorrect configuration settings, including use of relative DNS server name in failover/failback scripts, incorrect DNS server FQDN in failover/failback scripts (for example, use of secondary instead of primary DNS server FQDN), incorrect access credentials, and so on.	Warning	No

Validation Message	Error/ Warning	Auto-Fix Available?
“This machine may not be set up to use the correct DNS server.” This machine is set up to use a DNS server (xx.xxx.x.xx) that differs from the DNS server (xx.xxx.x.xx) where updates will be made. This can cause serious connectivity issues during and after failover and failback. Verify the client machine’s configuration, or modify the DNS server where updates will be made.	Warning	No
Identity failover		
“Identity failover is not recommended across different subnets” You have selected Identity failover. However, since the source and target are on different subnets, the source IP address will not be accessible after failover occurs. DNS failover is recommended for this configuration.	Warning	No
“Identity failover cannot be enabled unless at least one IP address is selected to be monitored” You have selected Identity failover, but no IP addresses are selected to be monitored. From the main Application Manager window, click **Configure**, then click **Configure** for Identity failover.	Error	No
Advanced options		
“The Create Repset option has been disabled” The Create Repset option has been disabled for this connection. This option should only be disabled for debugging purposes, and disabling it will prevent the proper setup of SQL protection. To enable the Create Repset option, select the **Fix** button.	Warning	Yes
“The Create Connection option has been disabled” The Create Connection option has been disabled for this connection. This option should only be disabled for debugging purposes, and disabling it will prevent the proper setup of SQL protection. To enable the Create Connection option, select the **Fix** button.	Warning	Yes
“The Create Failover Monitor option has been disabled” The Create Failover Monitor option has been disabled for this connection while failover is enabled. This option should only be disabled for debugging purposes, and disabling it will prevent the proper setup of failover monitoring. To enable the Create Failover Monitor option, select the **Fix** button.	Warning	Yes
“The Create Failover Scripts option has been disabled” The Create Failover Scripts option has been disabled for this connection while failover is enabled. This option should only be disabled for debugging purposes, and disabling it will prevent the proper setup of failover monitoring. To enable the Create Failover Scripts option, select the **Fix** button.	Warning	Yes
Services		
“Unable to connect to source server `<Source Server Name>` to get service information” The source server could not be contacted in order to get service information. This information is needed to determine whether SQL services are running on the source, which could cause problems with protection. Make sure you have sufficient rights to access the server. This message is displayed only once— not for each service.	Error	No
“Unable to connect to target server `<Target Server Name>` to get service information” The target server could not be contacted in order to get service information. This information is needed to determine whether SQL services are running on the target, which could cause problems with protection. Make sure you have sufficient rights to access the server. This message is displayed only once— not for each service.	Error	No
“Service `<Service Name>` is currently running on the target” The designated service is running on the target. This may prevent data from being written to the target, as the service may lock certain files. The service should be stopped on the target before enabling protection.	Error	Yes

Validation Message	Error/ Warning	Auto-Fix Available?
"Service <Service Name> is currently set to start automatically on the target" The designated service is set to start automatically on the target server. If the target server is restarted, the service will be started which may prevent data from being properly protected as the service may lock certain files. The service should be set to start manually before enabling protection.	Warning	Yes
"Service <Service Name> could not be found on the target" The designated service is missing from the target server. If this service is not available at failover time, SQL or other applications may not start properly.	Error	No
Replication set		
"A non-SQL connection for the replication set exists" A non-SQL connection for the replication set to the target server exists. After a failover and failback, data in this replication set that has been modified on the target may be overwritten. It is recommended that you make this data part of the SQL replication set in the Configure Protection window, and disconnect this connection.	Warning	No
"No data selected for protection" You must select some data (i.e., databases) for protection. Without information on which data to protect, the replication set is currently empty. Return to **Configure Protection**, select **Advanced**, and either select databases to protect or change protection mode.	Warning	No
"The Checksum All option is not enabled on the server <Server Name>." The Checksum All option is not enabled on the designated server. For transactional databases such as Exchange or MS SQL Server, this option is required to ensure data integrity on failover.	Warning	Yes
DT COM		
"The file DTCOM.dll is not available on the server <Server Name>." The file DTCOM.dll is not available on the designated server. This DLL is required by the Application Manager. This DLL is provided with the Application Manager installation and should be copied to the server before continuing.	Error	Yes
"The file DTCOM.dll is not registered on the server <Server Name>." The file DTCOM.dll is not registered on the designated server. This DLL is required by the Application Manager. This DLL is provided with the Application Manager installation and should be registered on the server before continuing.	Error	Yes
"A later version of the file DTCOM.dll is available for the server <Server Name>." The file DTCOM.dll is not the latest version. The latest version is provided with the Application Manager installation, and should be copied to the server before continuing.	Error	Yes
CAPICOM		
"The file CAPICOM.DLL is not available on the server <Server Name>." The file CAPICOM.DLL is not available on the designated server. This utility is needed to encrypt credentials necessary to run the DNS Failover Utility. This dll is provided with the Application Manager installation and should be copied to the server before continuing.	Error	Yes
"The file CAPICOM.DLL is not registered on the server <Server Name>." The file CAPICOM.DLL is not registered on the designated server. This DLL must be registered to encrypt credentials necessary to run the DNS Failover Utility. This DLL is provided with the Application Manager installation and should be registered on the server before continuing.	Error	Yes
"A later version of the CAPICOM.DLL is available for the server <Server Name>." The file CAPICOM.DLL is not the latest version. The latest version is provided with the Application Manager installation and should be copied to the server before continuing.	Error	Yes

Validation Message	Error/Warning	Auto-Fix Available?
Backup device		
“The <Backup Device Name> backup device does not match.” The designated backup device does not match between the source and target SQL Servers. If possible, all SQL backup devices should match to ensure full functionality on failover. If the source backup device is a file, local or remote, then you must ensure that access to the same path is configured on the target to guarantee that backups are performed successfully.	Warning	No
“The <Backup Device Name> backup device does not exist on the target.” The designated backup device does not exist on the target SQL Server. If possible, all source SQL Server backup devices should also exist on the target SQL Server to ensure full functionality on failover. If the source backup device is a file, local or remote, then you must ensure that access to the same path is configured on the target to guarantee that backups are performed successfully.	Warning	No
“The SQL Server backup devices are different.” The SQL Server backup devices are different between the source and target SQL Servers. If possible, all SQL Server backup devices should match to ensure full functionality on failover.	Warning	No
“Identity failover is not recommended” The Identity failover method cannot be used with integrated failover and failback. DNS failover can be used with integrated failover and failback, reduces downtime, and provides other benefits. It is recommended for most environments.	Warning	No
“Target Storage Mirroring service account does not have permissions to update the source SQL Server service SPNs on failover” The target Storage Mirroring service account does not have sufficient privilege within the domain to update the source SQL Server service SPNs on failover.	Error	Yes
NSISPN		
“The file NSISPN.exe is not available on the server <Server Name>.” The file NSISPN.exe is not available on the designated server. This utility is needed to modify the source and target SQL Service Principal Names (SPN) during failover and failback. This executable is provided with the Application Manager installation and should be copied to the server before continuing.	Error	Yes
“A later version of the NSISPN.exe is available for the server <Server Name>.” The file NSISPN.exe is not the latest version. The latest version is provided with the Application Manager installation and should be copied to the server before continuing.	Error	Yes
Source/target compatibility		
“The <Configuration Value Name> configuration value does not match.” The designated configuration value does not match between the source and target SQL Servers. If possible, all SQL Server configuration values should match to ensure full functionality and data integrity on failover.	Warning	Yes
“The <Configuration Value Name> configuration value does not exist on the target.” The designated configuration value does not exist on the target SQL Server. If possible, all source SQL Server configuration values should also exist on the target SQL Server to ensure full functionality and data integrity on failover. If you are protecting a SQL 2000 source with a SQL_2005 target, the configuration values will not match. You can ignore this message.	Warning	No
The <Configuration Value Name> configuration value does not exist on the source SQL Server.” The designated configuration value does not exist on the source SQL Server. A target SQL Server configuration value that does not also exist on the source SQL Server might impact functionality and data integrity on failover. If you are protecting a SQL 2000 source with a SQL_2005 target, the configuration values will not match. You can ignore this message.	Warning	No

Validation Message	Error/ Warning	Auto-Fix Available?
“The SQL Server configuration values are different.” The SQL Server configuration values are different between the source and target SQL Servers. If possible, all SQL Server configuration values should match to ensure full functionality and data integrity on failover.	Warning	Yes
“The Full Text Service configuration does not match.” The Full Text Service configuration does not match between the source and target SQL Servers. All SQL Server configuration values should match to ensure full functionality and data integrity on failover.	Error	Yes
“The integrated security configuration does not match.” The integrated security configuration does not match between the source and target SQL Servers. All SQL Server configuration values should match to ensure full functionality and data integrity on failover.	Error	Yes
“The job server configuration does not match.” The job server configuration does not match between the source and target SQL Servers. All SQL Server configuration values should match to ensure full functionality and data integrity on failover.	Warning	Yes
“The language configuration does not match.” The language configuration value does not match between the source and target SQL Servers. All SQL Server configuration values should match to ensure full functionality and data integrity on failover.	Warning	Yes
“The linked server configuration does not match.” The linked server configuration value does not match between the source and target SQL Servers. All SQL Server configuration values should match to ensure full functionality and data integrity on failover.	Warning	Yes
“The `<Linked Server Name>` linked server does not exist on the target.” The designated linked server does not exist on the target SQL Server. All source SQL Server linked servers should also exist on the target SQL Server to ensure full functionality and data integrity on failover.	Warning	No
“The `<User Name>` login configuration does not match.” The `<User Name>` login does not match between the source and target SQL Servers. All SQL logins should match to ensure full functionality on failover.	Error	Yes
“The `<User Name>` login does not exist on the target.” The `<User Name>` login does not exist on the target SQL Server. All source SQL Server logins should also exist on the target SQL Server to ensure full functionality and data integrity on failover.	Error	Yes
“The SQL Server logins are different.” The SQL Server logins are different between the source and target SQL Servers. If possible, all source SQL Server logins should exist on the target to ensure full functionality on failover.	Warning	Yes
“The `<Registry Value Name>` registry value does not match.” The designated registry value does not match between the source and target SQL Servers. All SQL Server registry values should match to ensure full functionality and data integrity on failover. If this registry value is not fixable, a message will appear stating that this registry value issue is not fixable in this version of the Application Manager. You must manually fix this issue.	Error	Varies
“The `<Registry Value Name>` registry value does not exist on the target.” The designated registry value does not exist on the target SQL Server. All source SQL Server registry values should also exist on the target SQL Server to ensure full functionality and data integrity on failover. If you are protecting a SQL 2000 source with a SQL_2005 target, the registry values will not match. You can ignore this message.	Warning	No

Validation Message	Error/ Warning	Auto-Fix Available?
“The <Registry Value Name> registry value does not exist on the source SQL Server.” The designated registry value does not exist on the source SQL Server. A target SQL registry value that does not also exist on the source SQL Server might impact functionality and data integrity on failover. If you are protecting a SQL 2000 source with a SQL_2005 target, the registry values will not match. You can ignore this message.	Warning	No
“The SQL Server registry values are different.” The SQL Server registry values are different between the source and target SQL Servers. If possible, all SQL Server registry values should match to ensure full functionality and data integrity on failover.	Warning	Yes
“The SQL Server startup parameters do not match.” The SQL Server startup parameters do not match between the source and target SQL Servers. All SQL Server startup parameters should match to ensure full functionality and data integrity on failover.	Error	Yes
“The remote server configuration does not match.” The remote server configuration value does not match between the source and target SQL Servers. All SQL Server configuration values should match to ensure full functionality and data integrity on failover.	Warning	Yes
“The <Server Name> remote server does not exist on the target.” The designated remote server does not exist on the target SQL Server. All source SQL Server remote servers should also exist on the target SQL Server to ensure full functionality and data integrity on failover.	Warning	No
“The SQL Server replication configuration does not match.” The SQL Server replication configuration value does not match between the source and target SQL Servers. All SQL Server configuration values should match to ensure full functionality and data integrity on failover.	Warning	Yes
“The <Server Role Name> server role member (<Server Role Member Name>) does not exist on target.” The designated source server role contains a member that does not exist as a member of the target SQL Server server role. All SQL Server server roles should match to ensure full functionality on failover.	Warning	No
“The <Server Role Name> server role does not exist on the target.” The designated server role does not exist on the target SQL Server. All source SQL Server server roles should also exist on the target SQL Server to ensure full functionality and data integrity on failover.	Warning	Yes
“The SQL Server server role configurations are different.” The SQL Server server role configurations are different between the source and target SQL Servers. If possible, all SQL Server server roles should match to ensure full functionality on failover.	Warning	Yes
“Source and target logical disk configurations don’t match” The protection mode you have selected requires that the target SQL Server has logical drives similar to the source. The designated drives contain source data, but do not exist on the target server.	Error	No
SQL database		
“The <Target Database Name> target database is online.” The target database (<Target Database Name>) is online and must be taken offline before protection can be enabled. Mirroring and replication will be unable to complete if a target file is kept open by an online database.	Error	Yes

Validation Message	Error/ Warnin g	Auto-Fix Available?
"The `<Source Database Name>` database user `<User Name>` does not exist on the target." The source database (`<Source Database Name>`) contains a user (`<User Name>`) that does not exist in the target SQL Server database. All SQL Server database users should match to ensure full functionality on failover.	Warning	Yes
"The `<Source Database Role>` database role member (`<Source Member>`) does not exist on the target." The source database <database name> role contains a member that does not exist as a member of the target SQL Server database role. All SQL Server database roles should match to ensure full functionality on failover.	Warning	Yes
"The SQL Server database configurations are different." The SQL Server database configurations are different between the source and target SQL Servers. If possible, all SQL Server users and roles should match to ensure full functionality on failover.	Warning	Yes
SQL language		
"The `<Language Name>` language does not exist on the target." The designated language does not exist on the target SQL Server. All source SQL Server languages should also exist on the target SQL Server to ensure full functionality and data integrity on failover.	Warning	No

Appendix E: Using the DNS Failover (DFO) Utility

The DNS Failover utility (`dfo.exe`), which is part of the Exchange Failover utility installation, can be used in the failover and failback scripts to delete and add host and reverse lookup entries so that the source host name will resolve to the target IP address.

For example, the following command could be executed from a command line or included in a batch file:

```
“c:\Program Files\StorageMirroring\dfo.exe” /dnssrvname dnsserver_name /srcname
source_name /srcip source_ip /tarname target_name /tarip target_ip /verbose
```

DNS Failover Utility Command Syntax

Command	`dfo`
Description	Used in script files to failover the DNS server name

Syntax	`dfo [/dnssrvname [dnsservername] /srcname [sourceFQDN]`
	`/srcip [sourceip] /tarip [targetip]`
	`/tarname [targetFQDN] /recordtype [recordtype]`
	`/username [username] /password [password]`
	`/dnszone [dnszonename] /dnsdomain [dnsdomainname]`
	`/logfile [logfilename] /failback [fbswitch]`
	`/setpassword [username] [password] /getpassword`
	`/trustee [trusteename] /verbose /test /debug /? | /help ]`

Options	• **`dnsservername`**—The name of the source domain/zone's primary DNS server (optional; local machine name used if missing) • **`sourceFQDN`**—The source machine's Fully Qualified Domain Name (required for modify) • **`sourceip`**—The source machine's IP address (required for modify) • **`targetip`**—The target machine's IP address (required for modify) • **`targetFQDN`**—The target machine's Fully Qualified Domain Name (required for modify on failback) • **`recordtype`**—The type of DNS resource records to modify or list (optional). Values can be: **`ALL`** (default), **`MSEXCHANGE`**, **`A`**, **`CNAME`**, **`MX`**, or **`PTR`** • **`username`**—The user account's domain name (optional; the account running the program is used if missing) • **`password`**—The user account's password (optional) • **`dnszonename`**—The name of the DNS zone or DNS container, used to refine queries (optional) • **`dnsdomainname`**—The name of the DNS domain, used to refine queries (optional) • **`logfilename`**—The name of the log file (optional) • **`fbswitch`** (optional)—By default, the DFO will only failback records in the `dfo_failback_config.dat` file. `fbswitch` allows you to enter a search criteria to identify the records to change back, even if they are not in the configuration file. `fbswitch` is also used if the `dfo_failback_config.dat` file is missing • **`trusteename`**—The domain account for the source server machine (`domain\machine$`). DFO attempts to deny write permissions to the DNS A record on failover for the account identified as the trustee. "Deny write permissions" is then removed from the DNS A record on failback. This keeps the source server from reclaiming its DNS A record if it comes back online prior to failback. • **`/failback`**—Denotes a failback procedure, performed after a failed source is recovered or restored (required for modify on failback) • **`/verbose`**—Logging and display level set to maximum detail (optional) • **`/test`**—Test mode. Modifications are not *actually* made, just listed (optional) • **`/debug`**—Forces DFO to write the DNS resource record as-is to the `dfolog.log` file prior to any DFO modify or list activity. • **`/?`**—Displays the syntax of the DNS Failover utility • **`/help`**—Displays the syntax of the DNS Failover utility
Password Encryption	• **`/setpassword`**—**NOTE:** This function must be run separate from a modify or list activity. `/setpassword` is designed to allow the user to store a username/password pairing in an encrypted file for later use. (optional, but required if `/getpassword` will be used) • **`/getpassword`**—Once a username/password pair has been encrypted and stored using `/setpassword`, this command can be used at the command line to retrieve the password associated with a specific username. It is designed to avoid storing passwords in clear text. (optional)

General Examples	• `dfo /dnssrvname mydns.mydomain.com /srcname mysource.mydomain.com /srcip 206.31.4.10 /verbose` Lists all resource records on the specified DNS server that match the source criteria • `dfo /dnssrvname mydns.mydomain.com /srcname mysource.mydomain.com /srcip 206.31.4.10 /tarip 210.11.12.13 /verbose` Modifies all resource records on the specified DNS server that match the source criteria, using the credentials of the account running the program to connect to the DNS server • `dfo /dnssrvname mydns.mydomain.com /srcname hasource.hadomain.com /srcip 210.11.12.13 /tarname mysource.mydomain.com /tarip 206.31.4.10 /failback /verbose` Modifies (fails back) all resource records on the specified DNS server that were changed on failover • `dfo /dnssrvname mydnsserver.mydomain.com /srcname mysource.mydomain.com /srcip 206.31.4.10 /tarip 210.11.12.13 /username mydomain.com\admin /password pword /verbose` Modifies all resource records on the specified DNS server that match the source criteria, using the username and password to connect to the DNS server
Password Encryption Examples	• `dfo /setpassword mydomain.com\admin mypassword` Stores the username (`mydomain.com\admin`) and password (`mypassword`) in the default credentials file (`dfo_credentials.dat`) • `dfo /dnssrvname mydnsserver.mydomain.com /srcname mysource.mydomain.com /srcip 206.31.4.10 /tarip 210.11.12.13 /username mydomain.com\admin /getpassword /verbose` Modifies all resource records on the specified DNS server that match the source criteria, using the username and `/getpassword` to retrieve the correct password for connecting to the DNS server

Appendix F: Using the Exchange Failover (EFO) Utility

There are several options available in the Exchange Failover utility for configuring Exchange for failover and failback. These options and the full command syntax are described in the following table.

Exchange Failover Utility Command Syntax

Command	**exchfailover**
Description	Used in script files to failover Exchange data
Syntax	**EXCHFAILOVER -FAILOVER | -FAILBACK -s <*source*> -t <*target*> [-l <*log_filename*>] [-norus] [-noRM] [-noRGconnectors] [-nospn] [-nooab] [-nopublicfolders] [-onlypublicfolders] [-noexchangeab] [-movehostspn] [-noADreplication] [-o <*options_filename*>] [-r [<*source_group*>] [,<*source_mail_store*>][:[<*target_group*>] [,<*target_mail_store*>]]] [-setup] [-test] [-u <*username*>:<*password*>] [-?[?]]**
Options	• **FAILOVER**—The Exchange data will be moved from the source to the target during failover • **FAILBACK**—The Exchange data will be moved from the target to the source during failback • **s** *source*—The name of the original source server • **t** *target*—The name of the original target server • **l** *log_filename*—The name of the optional log file name. By default, the log file is ExchFailover.log and is stored in the directory containing the exchfailover.exe file. If this name is changed, the DTInfo utility will not be able to locate this file which could impede assistance through Technical Support. • **norus**—Do not change the Recipient Update Service • **noRM**—Do not change the Routing Master • **noRGconnectors**—Do not change the Routing Group connectors • **nospn**—Do not change the Service Principal Name • **nooab**—Do not change the siteFolderServer for the offline address book • **nopublicfolders**—Do not move the public folders • **onlypublicfolders**—Only move the public folders • **noexchangeab**—Do not fail back the ExchangeAB SPNs for Small Business Server • **movehostspn**—Move the HOST SPN to/from the target instead of removing/adding it on the source • **noADreplication**—Do not force Active Directory replication of changes • **o** *options_filename*—Allows you to pass in a file containing the options for the Exchange Failover utility • **r**—By itself, this option creates a one-to-one mapping of the groups and mail stores from the source to the target • **r** *source_group*:*target_group*—The r option with the group names will direct the source group name specified to the target group name specified • **r** *source_group*, *source_mail_store*:*target_group*, *source_mail_store*—The r option with all of the r options will direct the source group name and mail store specified to the target group name and mail store specified • **setup**—Allows you to set the overwrite database on restore flag without completing user moves or RUS and folder updates. If the -setup switch is not supplied, the utility still sets the overwrite database on restore flag, but the other work is performed also. • **test**—Test mode that does not change the Exchange configuration • **u** *username*:*password*—A user with Active Directory permissions • **?**—Displays the syntax of the Exchange Failover utility • ??—Displays the syntax of the Exchange Failover utility along with brief descriptions of each option

Examples	• `exchfailover -failover -s Indy -t ExchSrvr_Bkup` • `exchfailover -failover -s Indy -t ExchSrvr_Bkup -r` • `exchfailover -failover -s Indy -t ExchSrvr_Bkup -r Sales:Indy_Sales` • `exchfailover -failover -s Indy -t ExchSrvr_Bkup -r Sales, Inside:Indy_Sales, Inside -r Sales, Outside:Indy_Sales, Outside` • `exchfailover -failover -s Indy -t ExchSrvr_Bkup -r Sales:Indy_Sales -norus -u administrator:password` • `exchfailover -failover -s Indy -t ExchSrvr_Bkup -o options_file.txt`
Notes	• When using the `-failback` option, the source-related options pertain to your original source or what will become the new source, if the original source had to be replaced. The target-related options pertain to the target that is currently standing in for the source. • The password specified with the `-u` option is the only case-sensitive option in this command.